1/24/2011

RICOH

Technical Information:

Network Security White Paper

Document Version G.1.2

Product Code	Ricoh	Savin	Gestetner	Lanier
D017	Aficio MP 2550B	9025b	MP 2550B	LD425B
D018	Aficio MP 2550	9025	MP 2550	LD425B
D019	Aficio MP 3350B	9033b	MP 3350B	LD433B
D020	Aficio MP 3350	9033	MP 3350B	LD433
D084	Aficio MP 2851	9228	MP 2851	MP 2851/LD528
D085	Aficio MP 3351	9233	MP 3351	MP 3351/LD533
D009	Aficio MP 4000B	9040b	MP 4000B	LD040B
D011	Aficio MP 4000	9040	MP 4000	LD040
D012	Aficio MP 5000B	9050b	MP 5000B	LD050B
D013	Aficio MP 5000	9050	MP 5000	LD050
D091	Aficio MP 4001	9240	MP 4001	MP 4001/LD140
D092	Aficio MP 5001	9250	MP 5001	MP 5001/LD150
D014	Aficio MP C6000	C6055	MP C6000	LD260c
D015	Aficio MP C7500	C7570	MP C7500	LD275c
G179	Aficio SP 8200DN	MLP150DN	SP 8200DN	LP150dn

Copyright © 2011 RICOH Americas Corporation. All rights reserved.

NOTICE:

This document may not be reproduced or distributed in whole or in part, for any purpose or in any fashion without the prior written consent of Ricoh Company limited. Ricoh Company limited retains the sole discretion to grant or deny consent to any person or party.

All product names, domain names or product illustrations, including desktop images, used in this document are trademarks, registered trademarks or the property of their respective companies. They are used throughout this book in an informational or editorial fashion only. Ricoh Company, Ltd. does not grant or intend to grant hereby any right to such trademarks or property to any third parties. The use of any trade name or web site is not intended to convey endorsement or any other affiliation with Ricoh products.

The content of this document, and the appearance, features and specifications of Ricoh products are subject to change from time to time without notice. While care has been taken to ensure the accuracy of this information, Ricoh makes no representation or warranties about the accuracy, completeness or adequacy of the information contained herein, and shall not be liable for any errors or omissions in these materials. The only warranties for Ricoh products and services are as set forth in the express warranty statements accompanying them. Nothing herein shall be construed as constituting an additional warranty. Ricoh does not provide legal, accounting or auditing advice, or represent or warrant that our products or services will ensure that you are in compliance with any law. Customer is responsible for making the final selection of solution and technical architectures, and for ensuring its own compliance with various laws such as the Gramm-Leach-Bliley Act, the Sarbanes-Oxley Act and the Health Insurance Portability and Accountability Act (HIPAA).

Version	Issue Date	Revised item
G.1.0	7, 5, 2008	Initial release
G.1.1	2,23,2010	Added New Model Information
G.1.2	11,24,2010	Added SSL Features Information

NOTE:

Throughout this document you may see references such as 04A (2004 Autumn) or 05S (2005 Spring). You will only see an A (Autumn) or S (Spring) attached to the last two digits of a year.
These two seasons reflect the time period the machines were manufactured.

Target Readers:

1. All end users: The information contained in the document can be distributed to end users as long as you follow the restrictions outlined on page 2.The main target readers are IT Administrators. When distributing this document to end users, region specific information including model names must be modified.
2. The regional support and marketing staff of each regional company
3. The support and marketing staff of Ricoh Sales companies including Ricoh family group companies and their subsidiaries.
4. Technical support personnel (CEs) of dealers.

Terms:

The following terms are used in this document. Please familiarize yourself with them.

The products: This refers to the digital multifunction and printing devices covered by this document, as noted in the Model Cross Reference table. The term “the products” refers to all of these machines collectively.

Host Interface: This refers to the physical interface of the Ethernet board on “the products”.

SSL: SSL is a communication technology used for secure connections between 2 hosts. The primary goal of the SSL Protocol is to provide privacy and reliability between two communicating applications. SSL is layered on top of some reliable transport protocol (e.g., TCP). SSL allows the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before the application protocol transmits or receives its first byte of data.

SSH2 (Secure Shell) is intended as a replacement for rlogin, rsh, and rcp. Additionally, ssh provides secure X connections and secure forwarding of arbitrary TCP connections. Ricoh’s implementation of SSH is based on OpenSSH 3.9.

Model Cross Reference:

The products: This refers to the digital multifunction and printing devices covered by this document, as noted in the Model Cross Reference table. The term “the products” refers to all of these machines collectively.

Product Code	Ricoh	Savin	Gestetner	Lanier
D017	Aficio MP 2550B	9025b	MP 2550B	LD425B
D018	Aficio MP 2550	9025	MP 2550	LD425B
D019	Aficio MP 3350B	9033b	MP 3350B	LD433B
D020	Aficio MP 3350	9033	MP 3350B	LD433
D084	Aficio MP 2851	9228	MP 2851	MP 2851/LD528
D085	Aficio MP 3351	9233	MP 3351	MP 3351/LD533
D009	Aficio MP 4000B	9040b	MP 4000B	LD040B
D011	Aficio MP 4000	9040	MP 4000	LD040
D012	Aficio MP 5000B	9050b	MP 5000B	LD050B
D013	Aficio MP 5000	9050	MP 5000	LD050
D091	Aficio MP 4001	9240	MP 4001	MP 4001/LD140
D092	Aficio MP 5001	9250	MP 5001	MP 5001/LD150
D014	Aficio MP C6000	C6055	MP C6000	LD260c
D015	Aficio MP C7500	C7570	MP C7500	LD275c
G179	Aficio SP 8200DN	MLP150DN	SP 8200DN	LP150dn

NOTE: Parts of this document may not apply to some models. For example, printer models do not have scanners. Therefore some uses of RSH (for scanning) do not apply to these models.

Table of Contents:

1. Introduction 9

1-1 Port Based Network Services and Potential Security Issues 9

1-2 TELNET 10

1-2-1 Function Overview: 10

1-2-2 Potential Threats 10

1-2-3 Possibility of Acting as a Server for Relaying Viruses 10

1-2-4 Theft of Username and Password 10

1-2-5 Interception of network packets: 11

1-2-6 Brute force password crack: 11

1-2-7 Possibility of Successful DoS (Denial of Service) Attacks 11

1-2-8 Recommended Precautions 11

1-3 FTP 12

1-3-1 Function Overview 12

1-3-2 Potential Threats: 12

1-3-3 Recommended Precautions 13

1-4 SFTP (SSH2) 13

1-4-1 Function Overview 13

1-4-2 Destruction, Corruption and Modification of the File System or Kernel 14

1-4-3 Possibility of Acting as a Server for Relaying Viruses 14

1-4-4 Theft of Username, Password, and Device Information 14

1-4-5 Brute force password crack: 14

1-4-6 Theft of Print Data 14

1-4-7 Possibility of Successful DOS (Denial of Service) Attacks 14

1-4-8 Recommended Precaution 14

1-5 HTTP 15

1-5-1 Function Overview 15

1-5-2 Destruction, Corruption and Modification of the File System 15

1-5-3 Possibility of Acting as a Server for Relaying Viruses 15

1-5-4 Theft of Username and Password 15

1-5-5 Theft of Print Data 15

1-5-6 Recommended Precautions 16
1-6 HTTPS 16
1-6-1 Function Overview 16
1-6-2 Theft of Username and Password 16
1-6-3 Theft of Print Data 17
1-6-4 Recommended Precautions 17
1-7 SNMP v1/v2 17
1-7-1 Function Overview 17
1-7-2 Potential Threats and Recommended Precautions 18
1-7-3 Recommended Precautions 18
1-8 SNMP v3 19
1-8-1 Function Overview 19
1-8-2 Potential Threats and Recommended Precautions 19
1-8-3 Recommended precaution 20
1-9 SHELL (RSH/RCP) 20
1-9-1 Function Overview 20
1-9-2 Potential Threats and Recommended Precautions 20
1-9-3 Recommended Precautions 21
1-10 LPD 21
1-10-1 Function Overview 21
1-10-2 Potential Threats and Recommended Precautions 21
1-10-3 Recommended Precaution 22
1-11 IPP 22
1-11-1 Function Overview 22
1-11-2 Potential Threats and Recommended Precautions 22
1-11-3 Recommended Precaution 23
1-12 DIPRINT (RAW Print) 23
1-12-1 Function Overview 23
1-12-2 Potential Threats and Recommended Precautions 23
1-12-3 Recommended Precautions 24
1-13 SMB 24

1-13-1 Function Overview 24
1-13-2 Potential Threats and Recommended Precautions 24
1-13-3 Visibility on the Network 25
1-13-4 Recommended Precautions 25
1-14 MDNS 25
1-14-1 Function Overview 25
1-14-2 Potential Threats and Recommended Precautions 25
1-14-3 Recommended Precaution 25
1-15 H323hostcall/SIP 25
1-15-1 Function Overview 25
1-15-2 Potential Threats and Recommended Precautions 26
1-15-3 Recommended Precaution 26
1-16 SSDP 26
1-16-1 Function Overview 26
1-16-2 Potential Threats and Recommended Precautions 26
1-16-3 Recommended Precaution 26
1-17 WS-Device 27
1-17-1 Function Overview 27
1-17-2 Potential Threats and Recommended Precautions 27
1-17-3 Recommended Precaution 27
1-18 IPDS 28
1-18-1 Function Overview 28
1-18-2 Potential Threats and Recommended Precautions 28
1-18-3 Recommended Precaution 28
1-19 RHPP 29
1-19-1 Function Overview 29
1-20 OTHERS 29
2. Other Network Services 30
2-1 Wireless LAN 30
2-1-1 Overview 30
2-1-2 SSID Only 30

2-1-3 WEP 30
2-1-4 WPA 30
2-1-5 Potential Threats 31
2-1-6 WEP 31
2-1-7 WPA 31
2-1-8 Recommended Precautions 31
2-2 IPsec 32
2-2-1 Overview 32
2-2-2 Recommended Precautions 33
3. Appendix 35
3-1 Services Requiring Open TCP/UDP Ports 35
3-2 Related Protocols 37
3-2-1 Access Control 38
3-2-2 Access Control – Web Image Monitor 39
3-2-3 Login as Administrator 40
3-2-4 Access Control – mshell 43
3-2-5 Disabling Services 44
3-3 Disabling Services – Web Image Monitor 48
3-3-1 Disabling Services – mshell 49
3-3-2 HTTP/HTTPS settings 50
3-3-3 Permit SSL/TLS Communication 50
3-4 SNMP settings: 53
3-4-1 Web Image Monitor 53
3-5 Network > SNMP v3 54
3-6 Mshell 56
3-7 Administrator Account Settings 57
3-7-1 Web Image Monitor 57
3-8 Network Security Level Settings 58
3-8-1 Configuration 58
3-8-2 Description of the Levels: 59
3-9 Wireless LAN settings 60

3-9-1 Web Image Monitor 60
3-9-2 [IEEE802.11b Settings] 61
3-9-3 WEP 62
3-9-4 WPA 63
3-9-5 mshell 65
3-9-6 IPsec Settings 66
3-9-7 Web Image Monitor 66
4. Reference List 72

1. Introduction

This document describes potential network threats and recommended precautions for them.

The products have built-in network services for providing a variety of features for wired and wireless network clients, such as network scanning, printing or faxing, and also client services for accessing network servers running outside the products, such as an LDAP server, Netware server, or Mail server.

This document focuses on how-to protect against potential threats from external attacks.

As the products are designed for use inside an Intranet where network clients and servers are protected by firewalls, the products rely on the Intranet's security policy, like the security provided by other network servers and clients. However, some customers require more strict security levels for network devices, because potential threats from inside the firewalls are increasing, and some configurations even use a secure connection to the Internet as a part of the Intranet.

To satisfy these demands, the products are all evaluated by security scanning applications during development, and also are checked for known vulnerability issues reported by Internet security organizations, such as CERT Coordination Center (CERT/CC : HTTP:// www.cert.org/). Whenever we find security vulnerabilities in the products, we provide appropriate countermeasures.

1-1 Port Based Network Services and Potential Security Issues

Some MFP/LP services allow write access from network clients. Because of this, some customers may feel that the products are not secure. In fact, the products are secure and provide security measures against potential threats to specific services, but some of these measures can make the services unavailable. For example, disabling the LPD port will make the products unavailable to LPR clients.

Disabling all protocols that are not used is highly recommended. This can be done quickly using Network Security Levels (described in the Appendix section entitled "Network Security Level Settings"). The Network Security Level function can be used to expedite security configuration. Please refer to the Appendix section entitled "Description of the Levels" for information about the configuration and a description of each level.

We also recommend using the Access Control function for added security. Access Control is a list of “safe” client host addresses. Once Access Control is setup for specific IP addresses, the products will receive print or scan requests from the specified hosts only. Access Control can be applied to LPR printing, RSH/RCP access, Bonjour access, HTTP/HTTPS access, FTP printing, TCP raw printing (DIPRINT), SMB printing, IPP printing, scanning from DeskTopBinder. Access Control can also be used for WSD-printing, IPDS printing, and RHPP printing. For information on how to set up Access Control, please refer to the Appendix section entitled “Access Control”.

In the following sections, the potential threats and recommended precautions are given for each service. For added security, the recommended precautions should be accompanied by a firewall and Access Control.

1-2 TELNET

1-2-1 Function Overview:

The TELNET service provides a virtual terminal service in order to use the maintenance shell (mshell). It is compliant with RFC 854. The mshell uses TCP port 23 and provides a dedicated command interface for the following functions:

- Configuring network settings of the products from remote terminals
- Monitoring device status and settings from remote terminals
- Getting system logs from remote terminals

Unlike shell services for UNIX/Linux, the mshell provides a command interface for configuration purposes only. Access to the file system or kernel, or modifying system files inside the products is very unlikely.

1-2-2 Potential Threats

Destruction, corruption and modification of the file system and kernel.
The possibility of destruction, corruption or modification of the file system is very low.
The mshell only permits write-access to a subset of device settings.

1-2-3 Possibility of Acting as a Server for Relaying Viruses

This is not an issue. Neither the local file system nor a remote host can be accessed via the mshell.

1-2-4 Theft of Username and Password

The username and password used for telnet is the same as those used for Web Image Monitor.

1-2-5 Interception of network packets:

When accessing the products using TELNET, the username and password are sent in clear text, because the TELNET protocol itself does not support encryption. So if the username and password are intercepted, the possibility of unauthorized access and changes being made does exist.

1-2-6 Brute force password crack:

The RICOH network device can detect a high frequency of failed logins. If the number of login attempts exceeds a configured threshold, the device will send an e-mail to the administrator. All failed logins will be logged.

1-2-7 Possibility of Successful DoS (Denial of Service) Attacks

The RICOH network device can detect a high frequency of logins and delay responses to that user's login requests. The device will also send an e-mail to the administrator. The device will log this and a message showing that the device is currently under attack will be displayed in Web Image Monitor.

1-2-8 Recommended Precautions

The following are suggested precautions against threats to the embedded TELNET service.

Scenario 1: Basic security settings

Change the username and password from the default value to something difficult to guess and change it regularly.
The username and password are the same as those used for logging into Web Image Monitor in Administrator mode; therefore, changing the username and password for the mshell means changing them for Web Image Monitor's Administrator mode.

Scenario 2: High security policy

Close the TELNET port:
The TELNET port can be completely closed using Web Image Monitor. When TELNET is disabled, the services provided by the mshell will not be available. TELNET should only be opened in cases where a machine setting needs to be changed and cannot be changed any other way. Before logging in, the products should be removed from the network and connected to a single PC. After the setting is changed, TELNET should be immediately closed again and can rejoin the network.

1-3 FTP

1-3-1 Function Overview

The FTP (File Transfer Protocol) service is compliant with RFC 959. TCP port 20 is used for the FTP-data service and TCP port 21 is used for the FTP-control service. In order to work with the products, FTP clients must be compliant with RFC 959.
The following functions are provided by the FTP service.

- Submitting a print job
- Downloading the files listed in the table below
- Remote Firmware Updates

File name	Description	Attribute
Syslog	System log	Read-only
Stat	Printer Status	Read-only
Prnlog	Print log	Read-only
Info	Printer Information	Read-only
Help	Help	Read-only
Fax application files: These cannot be seen by users. rwx - - - - - -	Fax job log Fax counter Fax address book	SmartDeviceMonitor for Admin/Client is required to read these files.

RFU requires machine administrator privileges. When Web Smart Device Monitor is used for RFU, TCP port 10020/10021 is used to send firmware files via the FTP protocol. However, port 21 is used to negotiate the transfer. All 3 ports must be open. RFU is a proprietary process defined by Ricoh and is extremely difficult to emulate. However if a strict security policy is to be maintained, that port can be closed via TELNET.

1-3-2 Potential Threats:

Destruction, Corruption and Modification of the File System

Although the FTP service permits write-access, any files that are received by the printer are considered to be a print job or firmware.

When the embedded FTP server receives an executable file, the product prints a binary representation (garbage characters) of the data contained in the executable. As for firmware, a dedicated account and

password that are disclosed only to Service Technicians is required to input firmware to the printer using the FTP service. In addition, firmware is verified by checking the header for a digital signature before being used. It would be extremely difficult to make fake firmware. A downgrade (ie installing old unsigned firmware) is not allowed by rfu.

Possibility of Acting as a Server for Relaying Viruses

This is unlikely, although the FTP service permits write-access. All written data submitted via the FTP service is treated as a print job or firmware. Any executable would be printed as binary (garbage data).

Theft of Username and Password

Interception of network packets: The FTP username and the password are sent in clear text because the FTP protocol itself does not support encryption. In fact, a username and password are not even necessary when logging into an FTP session.

Brute force password crack:

The RICOH network device can detect a high frequency of failed logins. If the number of login attempts exceeds a configured threshold, the device will send an e-mail to the administrator. All failed logins will be logged.

Theft of Print Data

Interception of network packets: Using FTP, print data is not encrypted. If intercepted by a third party it is easily read.

Possibility of Successful DOS (Denial of Service) Attacks

The RICOH network device can detect a high frequency of logins and delay responses to the user's login requests. The device will also send an e-mail to the administrator. The device will create a log and a message showing that the device is currently under attack will be displayed in Web Image Monitor.

1-3-3 Recommended Precautions

Never use FTP, always use SFTP.

1-4 SFTP (SSH2)

1-4-1 Function Overview

The SFTP ("Secure File Transfer Protocol" or "SSH File Transfer Protocol") service provides the same functions as FTP. SFTP uses an SSH (Secure Shell) session over TCP port 22. The SSH provides the following feature: Data Encryption (Protects against interception or falsification).
For information about OpenSSH, please see: http://www.openssh.com/

1-4-2 Destruction, Corruption and Modification of the File System or Kernel

Although the SFTP service permits write-access, any files that are received by the printer are considered to be a print job or firmware. If the embedded SFTP server receives anything other than a digitally signed firmware file, the device will print a binary representation (garbage characters) of the data. A dedicated account and password is required to input firmware to the printer using the SFTP service. In addition, the firmware must be digitally signed.

1-4-3 Possibility of Acting as a Server for Relaying Viruses

Although the SFTP service permits write-access, any data written to the device (executable or otherwise) is treated as a print job and output as printed pages.

1-4-4 Theft of Username, Password, and Device Information

Using SFTP, all data including the username and password is encrypted using DES, 3DES or AES.

1-4-5 Brute force password crack:

The RICOH network device can detect a high frequency of failed logins. If the number of login attempts exceeds a configured threshold, the device will send an e-mail to the administrator. All failed logins will be logged.

1-4-6 Theft of Print Data

Interception of network packets: Using SFTP, all data sent over the connection is encrypted. Therefore, even if data is intercepted, it will be difficult for unauthorized parties to read.

1-4-7 Possibility of Successful DOS (Denial of Service) Attacks

The RICOH network device can detect a high frequency of logins and delay responses to that user's login requests. The device will also send an e-mail to the administrator. The device will create a log and a message showing that the device is currently under attack will be displayed in Web Image Monitor.

1-4-8 Recommended Precaution

The following are suggested precautions against threats to the SFTP service.
Scenario 1 Basic Security: Change the username and password from the default value to something difficult to guess and change them regularly.

1-5 HTTP

1-5-1 Function Overview

The HTTP (Hypertext Transfer Protocol) service provides web services. This service is compliant with RFC 1945. TCP port 80 is used for the HTTP service.
The following functions are provided by the HTTP server service.

- Web Image Monitor
- Document server access via DeskTopBinder.
- Retrieving counter/user information using User Management Tool in SmartDeviceMonitor for Admin/Client
- Access to the products' address book using Address Management Tool in SmartDeviceMonitor for Admin.
- Submission of a job by an IPP client.
- Providing job status to an IPP client.

NOTE: When logging into Web Image Monitor in Administrator mode, the user must enter the username and password. It is the same as the username and password used for the mshell.

1-5-2 Destruction, Corruption and Modification of the File System

Unlikely, executable files cannot be run on the products' web server.

1-5-3 Possibility of Acting as a Server for Relaying Viruses

Unlikely, without access to the file system this would be impossible.

1-5-4 Theft of Username and Password

Interception of network packets: When accessing Web Image Monitor, the password is BASE64 encoded. The password is not sent in clear text, but it is not particularly difficult to decode. Therefore, if the password is intercepted and decoded, the possibility of unauthorized access and changing of device settings does exist.

1-5-5 Theft of Print Data

Interception of network packets: Using IPP, print data is sent as clear text, but if intercepted by a third party it is easily read.

1-5-6 Recommended Precautions

The following are suggested precautions against threats to HTTP service.

Scenario 1: Basic security settings

Change the username and password from the default value to something difficult to guess and change them regularly.
The username and password are the same as those used for logging in to mshell; therefore, changing the username and password for Web Image Monitor's Administrator mode means changing them for the mshell as well.

Scenario 1: Standard security settings

Forward HTTP requests to HTTPS.
Whether all, some, or none of the HTTP requests received by the MFP are forwarded to HTTPS, depends on the settings (Please refer to the Appendix section entitle "HTTP/HTTPS Settings").

Scenario 2: High security policy

Close the HTTP port.
The HTTP port can be completely closed with mshell. In this case, both Web Image Monitor and IPP (Internet Print Protocol) are unavailable via HTTP. However, Web Image Monitor and IPP printing are still available via HTTPS.

Note: We recommend using HTTPS instead of HTTP whenever possible.

1-6 HTTPS

1-6-1 Function Overview

HTTPS is HTTP over SSL (Secure Socket Layer). HTTPS provides the same functions as HTTP.
HTTPS maintains higher security than HTTP because SSL provides the following features:

- Identity verification
- Data integrity verification
- Encryption potential threats and recommended precaution

1) Destruction, corruption or modification of the file system

The HTTPS service is designed to deny access to the file system and prevent executable files from being run.

1-6-2 Theft of Username and Password

When using HTTPS, all data including the username and password is encrypted using an encryption algorithm negotiated during the SSL handshake. This is safer than sending username and passwords encoded in Base 64 (using the HTTP).

1-6-3 Theft of Print Data

Interception of network packets: Using HTTPS, all data sent over the connection is encrypted. Therefore, even if data is intercepted, it will be extremely difficult to use.

1-6-4 Recommended Precautions

The following are suggested precautions against threats to the HTTPS service.

Scenario 1: Basic security settings

Change the user names and passwords from the default value to something difficult to guess and change them regularly.

Scenario2: High security settings

Disable the web service.
If it is not needed, Web Image Monitor can be disabled using the mshell. When web is set to 'Down', Web Image Monitor does not activate and the error "503 Service Unavailable" is displayed. Even when not in use, TCP port 443 stays open and is therefore HTTPS is available for IPP printing.

1-7 SNMP v1/v2

1-7-1 Function Overview

The SNMP service is embedded in the products, to provide a method of managing them on the network. This service is compliant with RFC 1157 for SNMP v1 and RFC 1902 for SNMP v2. UDP port 161 is used for the SNMP service and UDP port 162 is used for SNMP-traps.
The following functions use SNMP:

- Configuring the settings of the products.
- Monitoring the status of the products.
- Detecting errors affecting the products.
- Communicating with the client PC for Scanning using the TWAIN driver.

Although the SNMP service is not protected by a password, it is protected using unique community names and assigned access rights (read-only, read-write and trap) within those communities. Access rights allow users to read or modify data in the MIB embedded in the products.
Default settings of SNMP community names are follows:
Read-only: public
Read-Write: admin

1-7-2 Potential Threats and Recommended Precautions

Destruction, Corruption and Modification of the File System

The possibility of destruction, corruption or modification of the file system is very low.
SNMP permits write-access to network parameters only. Access to the file system or kernel is not permitted using SNMP.

Theft of Community Name

Community names are sent in clear text because of the specification of the protocol. Therefore, if intercepted, the community name is easily read.

Possibility of Unauthorized Parties Intercepting Device Information

The products do not respond with important information such as administrator password even if the SNMP client sends a get request for this information. Therefore, the security risk is low. However when accessing the products using SNMP, parameters are sent in clear text. The SNMP v1/v2 protocols do not support encryption.

1-7-3 Recommended Precautions

The suggested precautions against this threat are as follows.
Scenario 1:

Basic security settings - Change the community names from the default value to something difficult to guess and change them regularly.

NOTE: When the community name settings are changed in the agents, the community name settings in the management utilities must also be changed.

Scenario 2:

Standard security settings – Change the setting so that only ‘get’ access using SNMP v1/v2 is allowed (disable ‘set’ access from SNMP v1/v2).

Scenario 3:

High security settings - Disable the SNMP v1/v2 service
If it is not absolutely necessary, the SNMP service should be disabled via Web Image Monitor or the mshell.

Scenario 4:

Very high security settings - Close the SNMP port
If it is not absolutely necessary, the SNMP port should be closed via Web Image Monitor or the mshell.

NOTE1: Please refer to the Appendix section entitle “SNMP settings” for details about SNMP settings.

NOTE2: We recommend using the maximum level of security possible. SNMP v3 should always be used in cases where SNMP v1/v2 is not absolutely necessary. Utilities that do not support SNMP v3 will not be able to get device status unless SNMP v1/v2 is enabled. Therefore, these utilities will not work correctly if SNMP v1/v2 has been disabled. If your utility does not support SNMP v3 and only requires ‘get’ access to work (doesn’t make any changes to MFP settings), then we recommend security Level 2.

1-8 SNMP v3

1-8-1 Function Overview

SNMP v3 provides the same functions as SNMP v1/v2. SNMP v3 maintains higher security than SNMP v1 and v2 because SNMP v3 has the following features:
User Authentication
Data Encryption

1-8-2 Potential Threats and Recommended Precautions

Destruction, Corruption and Modification of the File System

SNMP only permits write-access to network parameters. Access to the file system or kernel is not allowed.

Theft of Username and Password

Interception of network packets: When using SNMP v3, the password is hashed using SHA1 or MD5. Brute force password crack: The RICOH network device can detect a high frequency of failed logins. If the number of login attempts exceeds a configured threshold, the device will send an e-mail to the administrator. All failed logins will be logged.

Possibility of Unauthorized Parties Intercepting Device Information

Interception of network packets: The products do not respond with important information such as administrator password even if the SNMP client sends a get request for this information. Therefore security risk is low. In addition the products encrypt other parameters. (Please refer to the Appendix section entitle “SNMP settings”).

Possibility of Successful DOS (Denial of Service) Attacks

The RICOH network device can detect a high frequency of logins and delay responses to the user’s login requests. The device will also send an e-mail to the administrator. The device will create a log and a message showing that the device is currently under attack will be displayed in Web Image Monitor.

1-8-3 Recommended precaution

Scenario 1:

Basic security settings - Change the usernames and password from the default value and the passwords for each user to something difficult to guess and change it regularly.

Scenario 2:

Standard security settings - Encrypt all data.

Scenario 3:

High security settings - Disable the SNMP v3 service.
If it is not absolutely necessary, the SNMP v3 service should be disabled via Web Image Monitor or the mshell.

Scenario 4:

Very high security settings - Close the SNMP v3 port.
If it is not absolutely necessary, the SNMP port should be closed via Web Image Monitor or the mshell.

1-9 SHELL (RSH/RCP)

1-9-1 Function Overview

The Remote shell (RSH/RCP) service provides the following functions via TCP port 514. This is typically used from a UNIX/Linux client.

- Printing jobs from RSH/RCP clients.
- Monitoring machine status and settings.
- Obtaining the print logs and the system logs.
- Transferring scan data to the Twain driver.

1-9-2 Potential Threats and Recommended Precautions

Destruction, Corruption and Modification of the File System

Access is read-only.

Possibility of Acting as a Server for Relaying Viruses

Because access is read-only, this situation is very unlikely.

Theft of Username and Password

All data is sent in clear text. However, no password is required for access to RSH/RCP. SFTP is recommended in most situations.

Theft of Print Data

Using RSH/RCP, print/scan data is sent as clear text. If intercepted by a third party it is easily read.

1-9-3 Recommended Precautions

To maintain a strict security policy, the RSH/RCP service can be disabled and the port for this service can be completely closed using Web Image Monitor or the mshell.

NOTE: This will prevent users from TWAIN scanning.
We recommend using SFTP instead of RSH/RCP whenever possible.

1-10LPD

1-10-1Function Overview

The LPD service is compliant with RFC 1179 and uses TCP port 515 for connections with an RFC 1179 compliant client. The following functions are provided by this service:

- Printing a job from LPR clients
- Monitoring the status of the printer and print queues from LPR clients.
- Deleting print jobs from the print queue by LPR clients.
- Potential threats and recommended precaution

1-10-2Potential Threats and Recommended Precautions

Possibility of Acting as a Server for Relaying Viruses

The LPD service treats all received data as print jobs. An executable file will print as garbage data.

Possibility of Successful DOS (Denial of Service) Attacks

The RICOH network device can detect a high frequency of logins and delay responses to that user's login requests. The device will also send an e-mail to the administrator. The device will create a log and a message showing that the device is currently under attack will be displayed in Web Image Monitor.

Theft of Username and Password

Interception of network packets: LPD does not have an authentication function; however, print data may contain authentication information. This information can be encrypted by the printer driver. Please refer to the user manual and driver help sections for more information about this method.

Theft of Print Data

Interception of network packets: Using LPR, print data is sent as clear text, if intercepted by a third party it is easily read.

1-10-3 Recommended Precaution

As stated above, there are not many threats that apply to the LPD port. However, if a strict security policy is to be maintained, the LPD service can be disabled and the port for this service can be completely closed using Web Image Monitor or the mshell.

NOTE: The best way to reduce the possibility of print data being intercepted is to use IPP over HTTPS or SFTP instead of LPR as the printing protocol.

1-11 IPP

1-11-1 Function Overview

The IPP (Internet Printing Protocol) service is used for Internet printing from IPP clients. This service is compliant with RFC 2565 and uses TCP port 631.

The following functions are provided by the IPP service.

- Submission of jobs by an IPP client.
- Job status returned to IPP client.

The IPP service can have up to 10 password protected user accounts for the IPP service. Both “BASIC” and “DIGEST” authentication are supported. “BASIC” authentication sends the username and password in clear text. “DIGEST” authentication is more secure with the username and password hashed.

Both authentication methods are selectable in Web Image Monitor and mshell.

IPP authentication can also be disabled. In this case, usernames and passwords are not authenticated (The default setting is “disabled”.).

1-11-2 Potential Threats and Recommended Precautions

Possibility of Acting as a Server for Relaying Viruses

The IPP service treats all received data as print jobs. If someone sends an executable file via the embedded IPP service, the product prints the file as garbage data.

Theft of Username and Password

Interception of network packets: When the client negotiates the connection with the MFP, the MFP can specify whether the connection uses digest-MD5 hashing for the username and password.

Theft of Print Data

Interception of network packets: Using IPP, print data is sent as clear text, if intercepted by a third party it is easily read.

1-11-3 Recommended Precaution

In order to maintain a strict security policy, we recommend the following precautions.

Scenario 1

Standard Security: IPP Authentication should be either “BASIC” or “DIGEST”. This can be configured in Web Image Monitor, the mshell or the operation panel
“DIGEST” authentication is more secure than “BASIC” because the username and the password are not sent in clear text.

Scenario 2

High Security: Close the IPP port (631/TCP).
If it is not absolutely necessary, the IPP port should be closed via Web Image Monitor or the mshell.
NOTE1: This only closes the IPP port. The IPP service is still available using HTTP or HTTPS.
NOTE2: HTTPS is recommended over HTTP or IPP.

1-12 DIPRINT (RAW Print)

1-12-1 Function Overview

The DIPRINT (Direct Print or RAW Print) service is Ricoh Company Ltd’s name for port 9100 communication. This service provides direct printing from remote terminals using TCP port 9100.

1-12-2 Potential Threats and Recommended Precautions

Possibility of Acting as a Server for Relaying Viruses

The DIPRINT service treats all received data as print jobs. An executable file submitted to the embedded DIPRINT service would be printed as garbage data.

Theft of Username and Password

Interception of network packets: Print data may contain authentication information. This information can be encrypted by the printer driver. Please refer to the user manual and driver help sections for more information about this method.

Theft of Print Data

Interception of network packets: Depending on device and driver settings, print data might be sent as clear text. In this case, if intercepted by a third party, it is easily read.

1-12-3 Recommended Precautions

If a strict security policy is needed, the DIPRINT port can be changed or closed using Web Image Monitor or the mshell.

NOTE: To reduce the possibility of print data being intercepted, please use HTTPS instead of DIPRINT to submit jobs.

1-13 SMB

1-13-1 Function Overview

The SMB service uses NBT (NetBIOS over TCP/IP) as its base layer.

The NBT service provides the NetBIOS service over TCP/IP instead of NetBEUI. Using this service, a remote host can access network services of the products by the NetBIOS name (Computer Name) instead of IP address. This service uses 3 ports, UDP port 137 for NetBIOS-NS (NetBIOS Name Service), UDP port 138 for NetBIOS-DGM (NetBIOS Datagram Service) and TCP port 139 for NetBIOS-SSN (NetBIOS Session Service). SMB (Server Message Block) over TCP/IP provides the following services:

- Browsing print servers from SMB clients
- Installing Point and Print drivers to clients
- Printing jobs from SMB clients
- Sending job queue information to SMB clients
- Sending notifications of job completion to SMB clients

1-13-2 Potential Threats and Recommended Precautions

Possibility of Successful DOS (Denial of Service) Attacks

The RICOH network device can detect a high frequency of logins and delay responses to the user's login requests. The device will also send an e-mail to the administrator. The device will create a log and a message showing that the device is currently under attack will be displayed in Web Image Monitor.
Theft of Username and Password
Interception of network packets: The SMB protocol has authentication but a guest account can be configured. Some print data may contain authentication information. The password can be encrypted by enabling the printer driver's encryption function before sending data to the MFP. Please refer to the user manual and driver help for more information about this function.

Theft of Print Data

Interception of network packets: Using SMB, print data is sent as clear text, if intercepted by a third party it is easily read.

1-13-3 Visibility on the Network

To protect the products from being browsed by unauthorized parties, NetBIOS-NS and NetBIOS-DGM services should be disabled using the mshell.

1-13-4 Recommended Precautions

Scenario 1

Standard Security: Use Point and Print only with digitally signed drivers.

Scenario 2

High Security: Disable SMB. Use only IPP (with ssl) to submit jobs.

1-14 MDNS

1-14-1 Function Overview

MDNS (Multicast DNS) is a way of using familiar DNS programming interfaces, packet formats and operating semantics, in a small network where no conventional DNS server has been installed.

The products only use MDNS for Bonjour. If Bonjour is not being used, this port can be closed.

1-14-2 Potential Threats and Recommended Precautions

Possibility of Unauthorized Parties Intercepting Device Information

This is a possibility. The products use MDNS to advertise services and device information. If this is a concern, please close the port.

1-14-3 Recommended Precaution

If a strict security policy is to be maintained, the MDNS service can be disabled and the port for this service can be completely closed using Web Image Monitor or the mshell. (If Bonjour is turned off, the MDNS port is closed automatically.)

1-15 H323hostcall/SIP

1-15-1 Function Overview

H323/SIP services are used to provide VoIP (Voice over IP) for IP-Fax. The H.323 hostcall service is compliant with ITU-T standards and uses TCP port 1720. The SIP service is compliant with RFC3261 and uses TCP/UDP port 5060.

1-15-2 Potential Threats and Recommended Precautions

Theft of Username and Password

The SIP protocol has an authentication function. However, the products do not support authentication using the SIP protocol. Therefore, the username and password are not included with data sent over this protocol.

Theft of Facsimile Data

Interception of network packets: Using IP-Fax, facsimile data is formatted for an ISDN connection and is not encrypted. If intercepted by a third party, it can be read.

1-15-3 Recommended Precaution

If a strict security policy is to be maintained, the TCP/UDP ports for H323hostcall (1720) and for SIP (5060) can be changed or closed. However, these services cannot be stopped.

1-16 SSDP

1-16-1 Function Overview

SSDP (Simple Service Discovery Protocol) is used for both advertising services and searching for services on UPnP network. SSDP uses UDP port 1900. If UPnP is not being used, this port can be closed.

1-16-2 Potential Threats and Recommended Precautions

Possibility of Unauthorized Parties Intercepting Device Information

The products use SSDP to advertise services and search for services. If this is a concern, the SSDP service should be disabled using Web Image Monitor or the mshell.

1-16-3 Recommended Precaution

If a strict security policy is to be maintained, the SSDP service can be disabled and the port for this service can be completely closed using Web Image Monitor or the mshell.

1-17 WS-Device

1-17-1 Function Overview

WS-Device ('Web Service' Device) is a Windows Vista standard. This service is compliant with 'Device Profile for Web Services (February 2006)'.

The following functions are provided by the WS-Device service.

- Advertising the existence of the printing service. (WS-Discovery)
- Printing jobs to a WS-Device client. (WS-Printer)
- Providing the printer status to other WS-Device clients. (WS-Eventing)
- Providing details about the device and available services. (WS-Transfer / WS-MetadataExchange)

This service uses the following TCP/UDP ports:
TCP/UDP 3702: Used for the device advertisement (WS-Discovery)
TCP 53000: Used for WS-Device (WS-Transfer / WS-MetadataExchange)
TCP 53001: Used for WS-Printer (WS-Printer / WS-Eventing)
If a strict security policy is to be maintained, the WS-Device service can be disabled and the port for this service can be completely closed using Web Image Monitor or the mshell.

1-17-2 Potential Threats and Recommended Precautions

Theft of Print Data

Interception of network packets: The WS-device encodes data but does not encrypt it. Print data is sent as clear text, if intercepted by a third party it is easily read.

Leakage of Device Information

The products use WS-Device to advertise services and allow the user to know the device status and to print documents. If you do not want to unauthorized parties to be aware of this information, the WS-Device service should be disabled using Web Image Monitor or the mshell.

1-17-3 Recommended Precaution

If a strict security policy is to be maintained, the WS-Device service can be disabled and the ports for this service can be completely closed using Web Image Monitor or the mshell.

1-18 IPDS

1-18-1 Function Overview

Intelligent Printer Data Stream (IPDS) is a structured field data stream. It allows both data and commands to be streamed to the printer via channels, controllers or any type of networking link, which supports the transparent transmission of data to print processes that are resident in the device.

This service uses following TCP/UDP port:
TCP 5001: Used for transmitting data and printer control commands.

1-18-2 Potential Threats and Recommended Precautions

The Possibility of Acting as a Server for Relaying Viruses

The IPDS service treats all received data as print jobs and job control commands.

Theft of Username and Password

Interception of network packets: IPDS print can not be authenticated by the printer. Therefore, there is no username and password in the IPDS print data.

Theft of Print Data

Interception of network packets: Using IPDS, print data is not encrypted. If intercepted by a third party, it is possible to read.

Possibility of Successful DOS (Denial of Service) Attacks

The RICOH network device can detect a high frequency of logins and delay responses to the user's login requests. The device will also send an e-mail to the administrator. The device will create a log and a message showing that the device is currently under attack will be displayed in Web Image Monitor.

1-18-3 Recommended Precaution

If a strict security policy is to be maintained, the IPDS service should not be installed. In addition, it can be disabled and the port for this service can be completely closed using Web Image Monitor or the mshell.

1-19 RHPP

1-19-1 Function Overview

Though MFPs of all regions support RHPP, Ricoh has not released any RHPP servers outside of Japan. We do not foresee the need for this service in the near future. Please close the ports.

This service uses the following TCP/UDP port: TCP 59100: Used for transmitting data and printer control commands.

NOTE: As of 2008, there are no RHPP print servers on the market outside of Japan.

1-20 OTHERS

TCP port 7443 and 7444 are reserved for @Remote. If a strict security policy is to be maintained, those ports can be closed via TELNET. (Please refer to the Appendix for a list of ports.)

HTTPS is used for this service as an underlying layer. Please refer to the “HTTPS” section for the potential threats and recommended precautions for HTTPS.

2. Other Network Services

The previous section dealt mainly with physical port based network services. This section will describe security related information for network services not based on physical ports.

2-1 Wireless LAN

2-1-1 Overview

WLAN utilizes spread spectrum technology based on radio waves to enable communication between devices in a limited area. This gives users the mobility to move around within a broad coverage area and still be connected to the network. The absence of cables leaves transmissions extremely susceptible to interception. For this reason a variety of security precautions have been incorporated into WLAN specifications.

2-1-2 SSID Only

All data is sent as clear text without any authentication or integrity checking. As wireless data is available to anyone within range, unencrypted data is extremely susceptible to tampering and theft.

2-1-3 WEP

'WEP' (Wired Equivalent Privacy) is a security standard settled on by IEEE, and adopted as IEEE802.11. Using WEP, data can be encrypted with a shared key (RC4). Access to the network is based on a WEP key configured on the client's computer and the access points. Although WEP provides a degree of security, it does have vulnerabilities. 'WPA' was created to overcome the vulnerabilities in WEP which supports the products.

2-1-4 WPA

'WPA' (WiFi Protected Access) is a subset of IEEE802.11i. It utilizes a key exchange system to constantly change the shared key. This re-keying can be done using either TKIP or CCMP. However, support for WPA2 is required for CCMP. TKIP uses RC4 as an encryption algorithm and is intended for use with legacy systems that do not yet support CCMP. In addition to providing key exchange, CCMP uses the AES encryption algorithm which is a stronger than RC4.

Encryption Method	WEP	WPA	
		TKIP	CCMP
Encryption Algorithm	RC4	RC4	AES
Shared Key Size	40/104 bit	104 bit	128 bit
Key Exchange / Refresh	No / No	Yes / Yes	

WPA employs four authentication modes: 'WPA-PSK', 'WPA2-PSK', 'WPA (802.1X)' and 'WPA2 (802.1X)'. WPA-PSK and WPA2-PSK are similar to WEP in that a pre-shared key is used to join the network. However, a new encryption key is generated in handshake process, making WPA-PSK and WPA2-PSK more secure than WEP. WPA (802.1X) and WPA2 (802.1X) are more strict than the PSK protocols. Only users that can be authenticated by a RADIUS server using EAP are allowed to join the network.
Supported EAP authentication types are:

- EAP-TLS
- EAP-TTLS
- PEAP
- LEAP

2-1-5 Potential Threats

SSID Only (No Encryption)

All data (including the SSID) is transmitted in plain text. It is easily readable by anyone within range of the wireless transmission.

2-1-6 WEP

WEP provides RC4 encryption of data and is therefore more secure than using only a SSID. However, the weakness of RC4 encryption and WEP are well documented.
NOTE: WPA TKIP uses RC4. However, because the keys are being constantly refreshed, the key will change before it can be cracked.

2-1-7 WPA

In WPA, the encryption key is generated at intervals by TKIP or CCMP. The key does not need to be entered manually. Since the key is refreshed often, a brute force attack is almost impossible. Furthermore, CCMP uses AES, which is a stronger encryption method than RC4. As an added precaution, WPA (802.1X) /WPA2 (802.1X) provides user authentication.

2-1-8 Recommended Precautions

Please take the appropriate action for your security policy.
Scenario 1:

Basic security settings:
General Access Point settings
Prohibit broadcast of the SSID.
Prohibit connections that do not have the correct SSID.
Limit connections to only specific MAC addresses.
We recommend not using security Level 1.

Scenario 2:

Standard security settings:
WEP
We recommend making regular changes to the PSK.

Scenario 3:

High security settings:
WPA-PSK/WPA2-PSK

Scenario 4:

Very high security settings:
WPA (802.1X)/WPA2 (802.1X) instead of WPA-PSK/WPA2-PSK.

Please refer to the Appendix section entitled “Wireless LAN Settings” for an explanation of how to configure these settings.

2-2 IPsec

2-2-1 Overview

Internet Protocol Security (IPsec) is a suite of protocols which provides secure communication over the network layer. IPsec provides authentication, data integrity, and protection against replay attacks. Unlike SSL which functions between the application and transport layers, IPsec functions in the network layer.

The products can offer the following header extensions.

AH

Authentication, integrity (IP header and the payload).
No encryption.

ESP

Authentication, encryption, (payload only)

AH+ESP

Authentication, encryption, (IP header and the payload)

The Ricoh implementations for the encryption and authentication algorithm are:

Encryption:
Clear Text (No encryption)
DES
3DES
AES-128
AES-192
AES-256

Authentication:
HMAC-MD5-96
HMAC-SHA1-96

The encryption or authentication keys can be set manually or generated automatically using IKE.

NOTE: IPsec are disabled for DHCP, DNS, WINS, and HTTPS by default. IPsec can be applied to these protocols by enabling it in mshell.

2-2-2 Recommended Precautions

The suggested precautions are as follows.
Key Exchange:

Use IKE instead of the manual key exchange. If the encryption or authentication keys have to be set manually, there will be no re-keying. The same keys will be used until manually changed again.

Security Protocol:

Scenario 1

Basic: AH
No encryption.
Selectable authentication algorithm.

Scenario 2

Standard: ESP
Payload is encrypted.
Selectable authentication algorithm.

Scenario 3

High: ESP+AH
Very secure.
Encryption of the payload and headers
Data integrity
Authentication
Please refer to the Appendix section entitled “IPSEC Settings” for an explanation of how to configure these settings.

3. Appendix

3-1 Services Requiring Open TCP/UDP Ports

Protocol	Port Num.	Login	Username Changeable	Password	Password Changeable	Note
TELNET	23/TCP	Y	Y	Y	Y	This is the same username and password as used for Web Image Monitor.
FTP-control	21/TCP	Y	N	N	N	For RFU, administrator privilege is required.
HTTP	80/TCP	Y	Y	Y	Y	This is the same username and password as used for TELNET. The unauthorized users only have read access.
netbios-ns	137/UDP	N	N	N	N	
netbios-dgm	138/UDP					
netbios-ssn	139/TCP					
SNMP	161/UDP	Y	Y	N	N	Although there is no concept of user accounts, it can perform access restrictions using the Community Name. Up to 10 Communities can be registered.
SNMPv3	161/UDP	Y	Y	Y	Y	This is the same username and password as used for TELNET. If no password is input, then only read access is available.
HTTPS	443/TCP	Y	Y	Y	Y	This is the same username and password as used for TELNET. If no password is input, then only read access is available.
RSH/RCP (shell)	514/TCP	N	N	N	N	
LPD	515/TCP	N	N	N	N	
IPP	631/TCP	Y	Y	Y	Y	Authentication by account/password is not performed by default. In this case, all users are ANONYMOUS. When IPP authentication is enabled, a username and password will be required.

Protocol	Port Num.	Login	Username Changeable	Password	Password Changeable	Note
H323gatestat	1719/UDP	N	N	N	N	If the products are configured to use ‘gatekeeper’, this port is opened so the products can register its information with gatekeeper.
H323hostcall	1720/TCP	N	N	N	N	
SSH	22/TCP	Y	Y	Y	Y	SSH is only used for SFTP. For RFU, administrator privilege is required. For SFTP, RFU is not available via Web Smart Device Monitor.
SIP	5060/TCP, UDP	N	N	N	N	The SIP protocol supports authentication. However, we do not support SIP authentication with our products.
MDNS	5353/UDP	N	N	N	N	
@Remote	7443/TCP 7444/TCP	-	-	-	-	
SSDP	1900/UDP	N	N	N	N	
DIPRINT	9100/TCP	N	N	N	N	
RFU	10021/TCP	Y	-	-	-	This port functions similarly to an FTP port and used for Web Smart Device Monitor.
WS-Printer	53001/TCP	N	N	N	N	
IPDS	5001/TCP	N	N	N	N	
RHPP	59100/TCP	N	N	N	N	

3-2 Related Protocols

Protocol	Protocol Suite	Commonly Used Port Num.	Description of the protocol's function in the Products.
IP	TCP/IP	-	-
ICMP	TCP/IP	Protocol Num. 1	-
UDP	TCP/IP	Protocol Num. 17	-
TCP	TCP/IP	Protocol Num. 6	-
FTP-data	TCP/IP	20/tcp, udp	1) Sending scan data to the FTP server. (Scan to FTP) 2) Sending scan data to ScanRouter
FTP-control	TCP/IP	21/tcp, udp	
SMTP	TCP/IP, IPX/SPX	25/tcp, udp	1) Sending scan data to the SMTP server. (Scan to E-mail)
Domain (DNS)	TCP/IP	53/tcp, udp	1) Resolving IP addresses from the server name.
BOOTP DHCP	TCP/IP	67/tcp, udp 68/tcp, udp	1) Getting IP addresses and other network parameters from the DHCP server.
POP	TCP/IP	110/tcp, udp	1) Using POP before SMTP authentication for 'Scan to E-mail'. 2) Receiving internet-fax data.
SNTP	TCP/IP	123/tcp, udp	1) Getting UTC from the NTP server.
NETBIOS-NS	TCP/IP, IPX/SPX, NetBEUI	137/tcp, udp	1) Sending scan data to SMB clients. (Scan to SMB)
NETBIOS-DGM		138/tcp, udp	
NETBIOS-SSN		139/tcp, udp	
IMAP	TCP/IP	143/tcp, udp	1) Getting internet-fax data
SNMP-trap	TCP/IP, IPX/SPX	162/tcp, udp	1) Sending status information to Network Management Server.
LDAP	TCP/IP	389/udp, tcp	1) Searching e-mail addresses from the LDAP server's address book.
syslog	TCP/IP	514/udp	1) Sending system logs to a syslog server.
NCP	TCP/IP, IPX/SPX	524/tcp, udp	1) Logging in to a Netware server. 2) Printing from the Netware environment.
SLP	TCP/IP	427/tcp, udp	1) Searching for a Netware Server.
IPX	IPX/SPX	-	1) Providing ipx connections
SPX	IPX/SPX	-	1) Providing spx connections
SAP	IPX/SPX	-	1) Broadcasts to availability of print services.

Protocol	Protocol Suite	Commonly Used Port Num.	Description of the protocol's function in the Products.
RIP	IPX/SPX	-	1) Broadcasts route information.
APPLETALK	APPLETALK	-	1) Providing appletalk connections.
PAP	APPLETALK	-	1) Providing appletalk printing services
NETBEUI	NETBEUI	-	1) Providing netbeui connections.
IKE	IPsec	500/udp	1) Providing IKE connections.

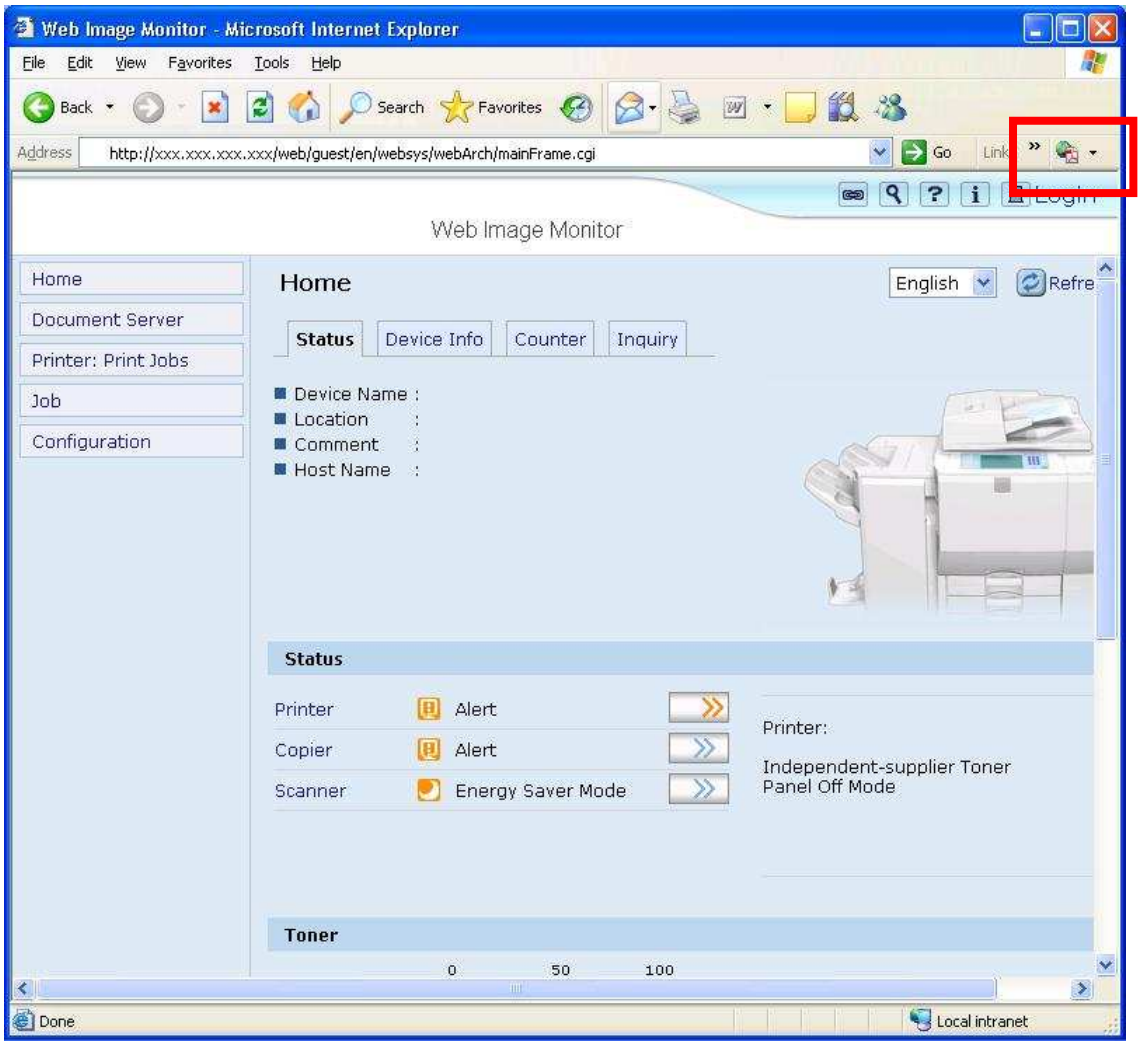
Commonly Used Port Number: This is meant to be general information. This column contains well-known port numbers commonly used in the industry. This is not necessarily the port used by the products.

3-2-1 Access Control

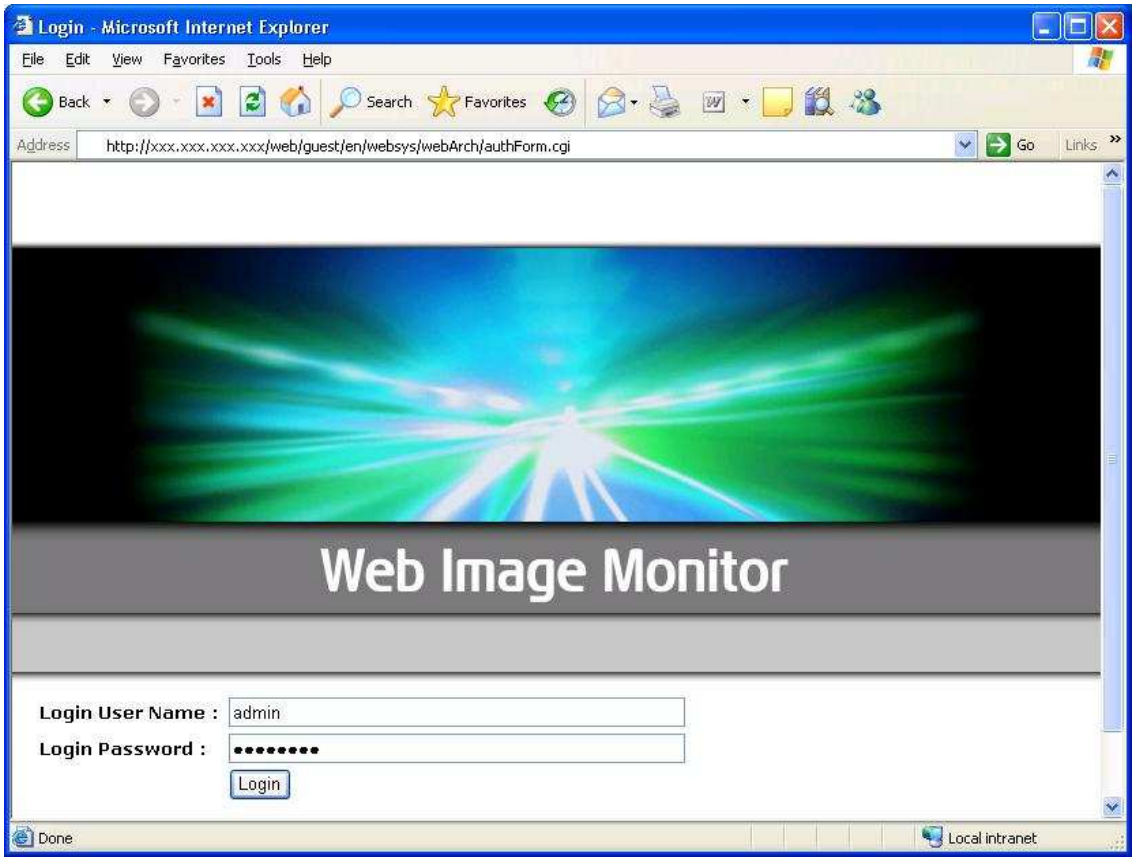
The printer will accept communication only from a set range of IP addresses. This can be applied to connections from LPR, RSH/RCP, HTTP, HTTPS, Bonjour, SSH/SFTP, FTP, DIPRINT, SMB, IPP, WS-Device, WS-Printer, IPDS, RHPP, and DeskTopBinder.
These cannot be applied to TELNET or SmartDeviceMonitor.

3-2-2 Access Control – Web Image Monitor

Web Image Monitor can be used for accessing the products. A supported Browser such as Microsoft Internet Explorer and the product's IP address is required.



3-2-3 Login as Administrator



The four administrator types are identified as follows:

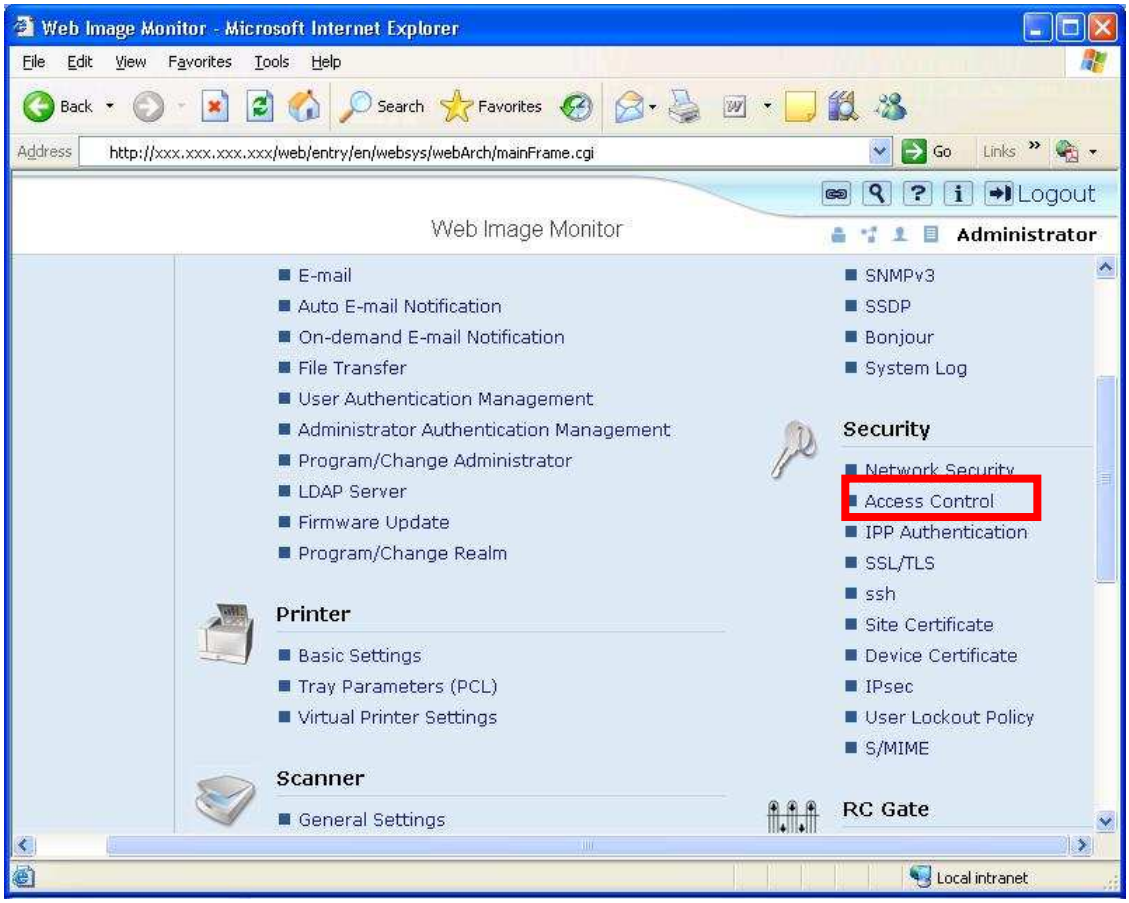
: Machine Administrator

: Network Administrator

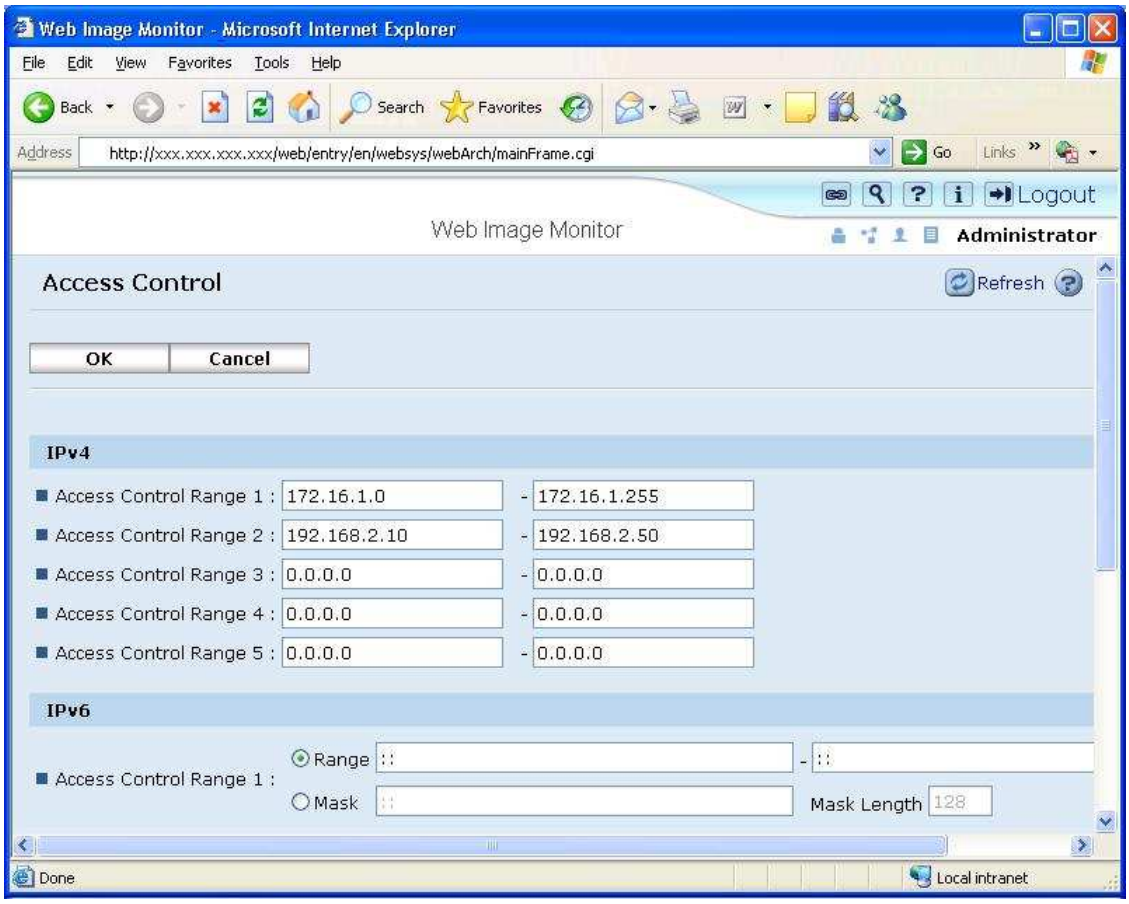
: User Administrator

: File Administrator

By default, all administrator privileges are merged into one administrator. If Admin Auth is enabled, then Network Administrator privileges are required in order to use Access Control.



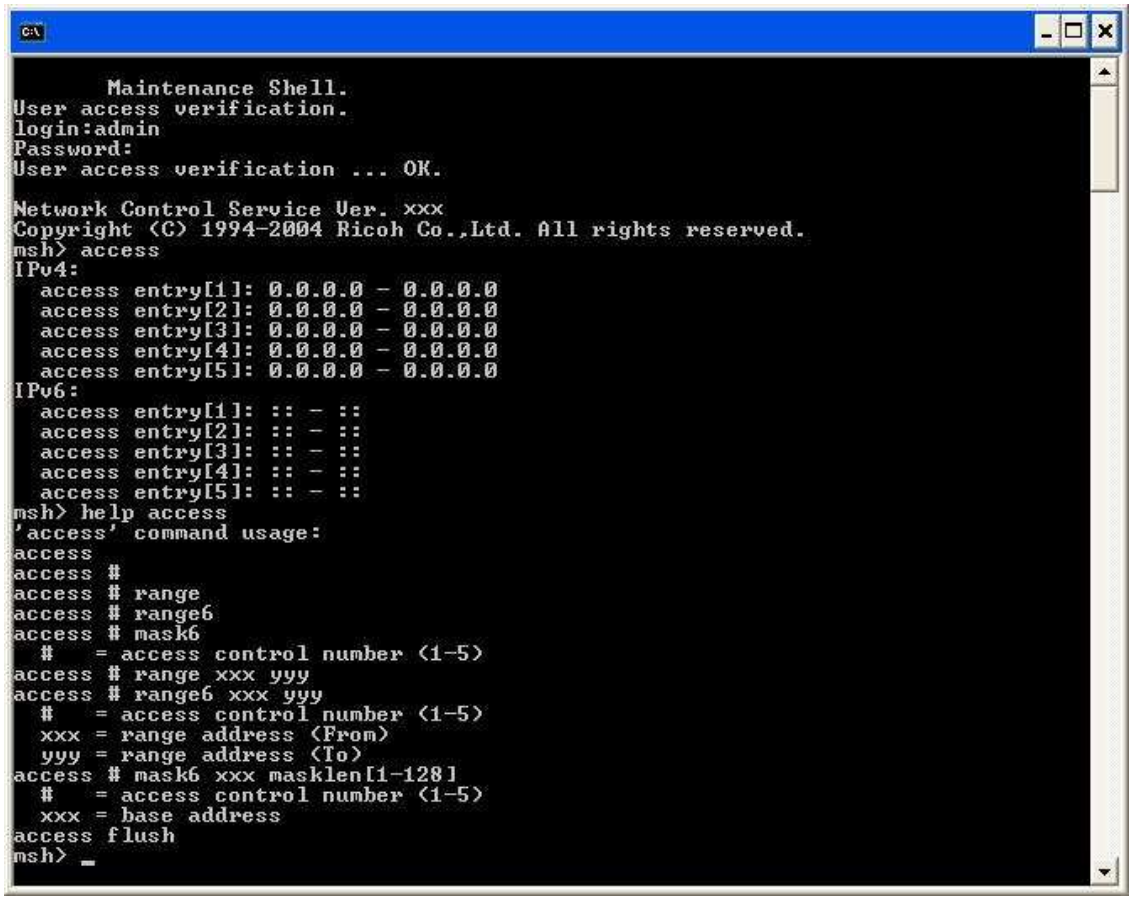
Input the range of IP addresses that you wish to permit communication.
Click the 'OK' button to commit the changes.



3-2-4 Access Control – mshell

The following example is shown using the Windows XP telnet client.

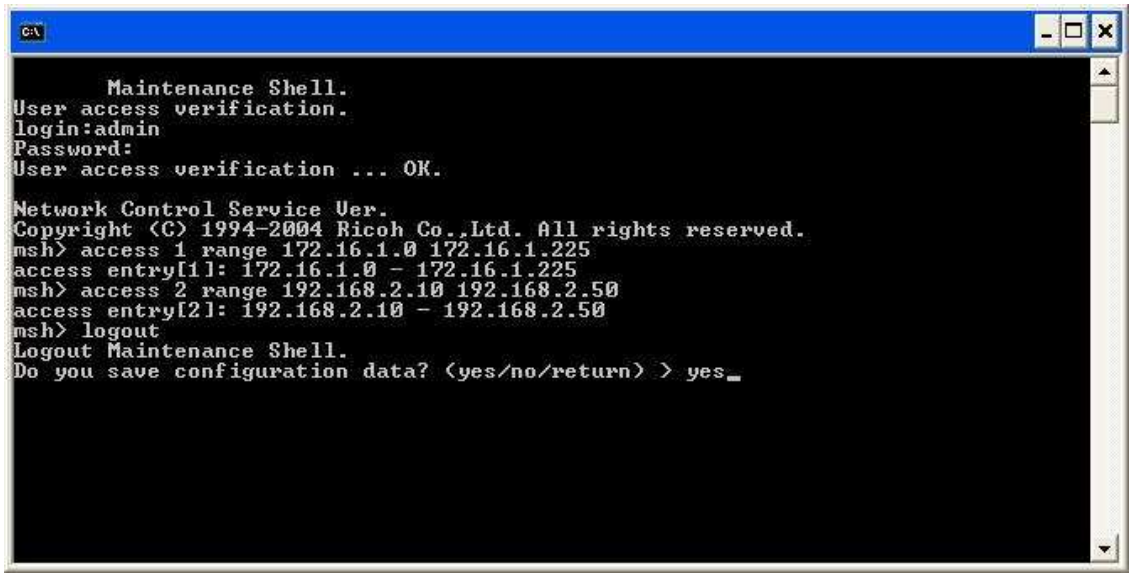
Telnet into the Maintenance Shell (mshell), a username and password will be required for this. Use the access command to input the access control range.



E.g.1 Input the following command to permit only access from 172.16.1.0 to 172.16.2.0:
msh> access 1 range 172.16.1.0 172.16.2.0

E.g.2 Input the following command to clear all access ranges:
msh> access flush

If changes have been made, the following question will appear when the user tries to logout. ‘Did you save configuration data?’ Input ‘yes’ to commit the changes, input ‘no’ to discard them.


Maintenance Shell.
User access verification.
login:admin
Password:
User access verification ... OK.
Network Control Service Ver.
Copyright (C) 1994-2004 Ricoh Co.,Ltd. All rights reserved.
msh> access 1 range 172.16.1.0 172.16.1.225
access entry[1]: 172.16.1.0 - 172.16.1.225
msh> access 2 range 192.168.2.10 192.168.2.50
access entry[2]: 192.168.2.10 - 192.168.2.50
msh> logout
Logout Maintenance Shell.
Do you save configuration data? (yes/no/return) > yes

3-2-5 Disabling Services

The following table describes whether services or ports can be opened or closed using Web Image Monitor and/or mshell.

See “Network Security Level Settings” for more information.

NOTE: Some ports cannot be closed via the above settings. See comments in table below.

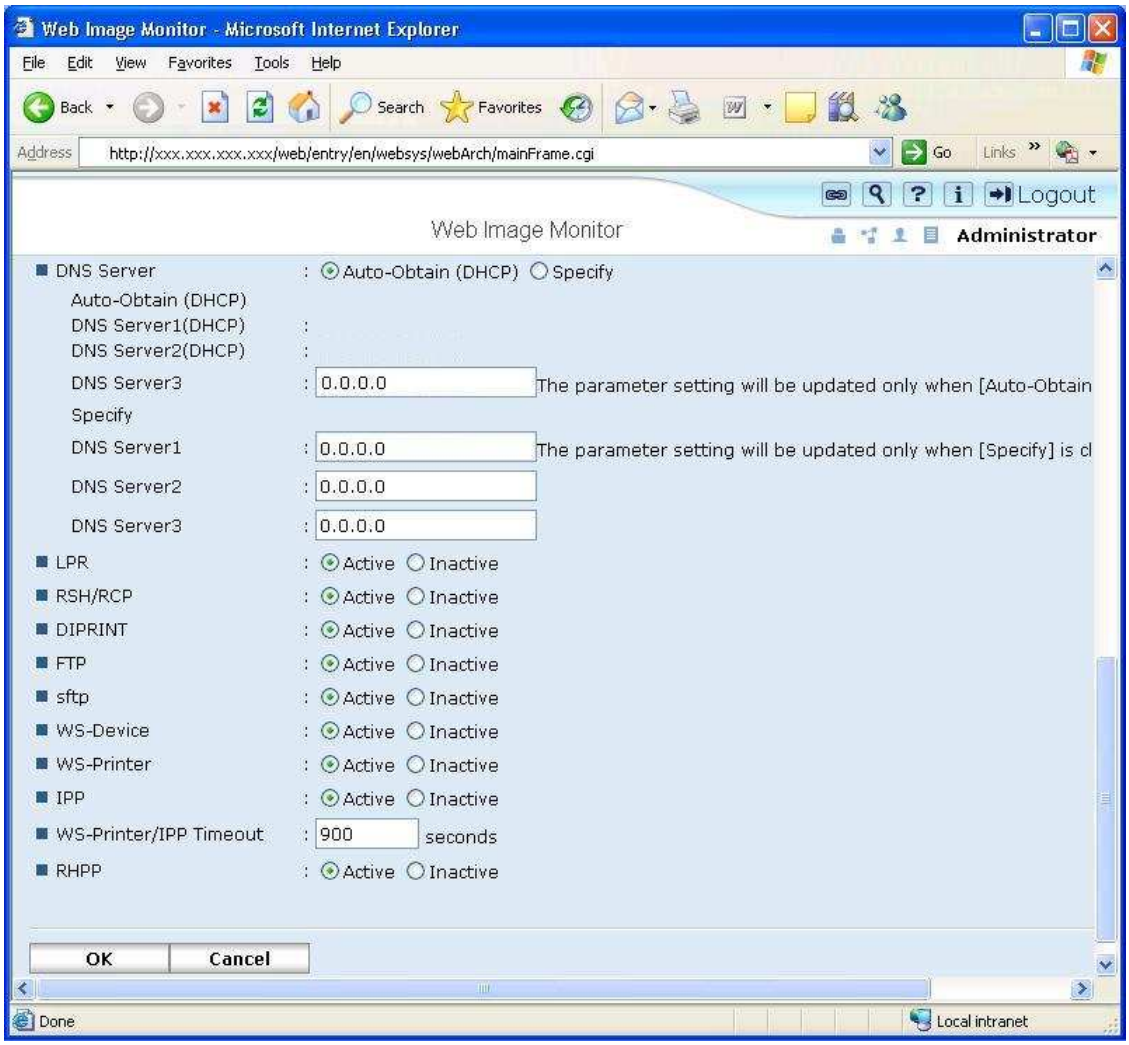
Service/Protocol	Port	Web Image Monitor		mshell		Comment
Netware	-	Y		Y		Setting Netware to down, disables the IPX/SPX protocol and NCP/IP. Therefore, if Netware is down, printing in the IPX/SPX environment and in the pure IP environment is unavailable. LPR in NDPS and iPrint (IPP Printing) are unaffected.
AppleTalk	-	Y		Y		
		IPv4	IPv6	IPv4	IPv6	
TCP/IP	-	Y	Y	Y	Y	It is not possible to set own TCP/IP version via Web Image Monitor. For example, in order to disable TCP/IPv4, it needs to be connected via TCP/IPv6.

FTP	21	Y	Y	Y	Y	Setting FTP to down closes FTP port (21/tcp). The FTP server service will be down but the FTP client function is still available. Therefore, if this function is down, Scan to FTP is still available.
SSH/SFTP	22	Y	Y	Y	Y	If either of ssh or sftp is set to down, this port will be closed.
TELNET	23	Y	Y	-	-	Telnet cannot be disabled via mshell for obvious reasons.
SMTP	25	Y	-	-	-	Configuration > E-mail > Reception Protocol > 'POP3' or 'IMAP4'.
HTTP	80	Y	Y	Y	Y	Setting 'web down' does not close this port. In order to close this port open mshell and type 'set http down'. In order to close this port via Web Image Monitor, it needs to be connected via HTTPS or IPv6.
IPP	631	Y	Y	Y	Y	
NBT	137/138	Y	-	Y	-	Setting NBT to down closes NetBIOS-NS (137/UDP) and NetBIOS-DGM (138/UDP)
SMB	139	Y	-	Y	-	Setting SMB to down closes NetBIOS-SSN (139/TCP).

SNMP	161	Y	Y	Y	Y	Use Web Image Monitor' to close this port. Setting SNMP to down closes SNMP port (161/udp). In addition when SNMP is down, the SNMP trap function and SNMP function over IPX/SPX is not available.
SSL	443	Y	Y	Y	Y	HTTP and HTTPS cannot both be closed at the same time from Web Image Monitor.
RSH/RCP	514	Y	Y	Y	Y	
LPR/LPD	515	Y	Y	Y	Y	
H.323	1720	Y	-	-	-	In order to close this port: Configuration > Fax > IP-Fax Settings > Enable H.323 > 'Off' (Web Image Monitor). This port cannot be closed via mshell.
SSDP	1900	Y	-	Y	-	Setting SSDP to down makes UPnP unavailable and closes the SSDP port (1900/UDP)
MDNS	5353	Y	-	Y	-	In order to close this port, set 'Bonjour' to down.
SIP	5060	Y	-	-	-	In order to close this port: Configuration > Fax > IP-Fax Settings > Enable SIP > 'Off' (Web Image Monitor). This port cannot be closed via mshell.
@Remote	7443/7444	-	-	Y	-	In order to disable this service, type 'set nrs down' in mshell.
DIPRINT	9100	Y	Y	Y	Y	If this port is closed, printing from diprint clients is unavailable.

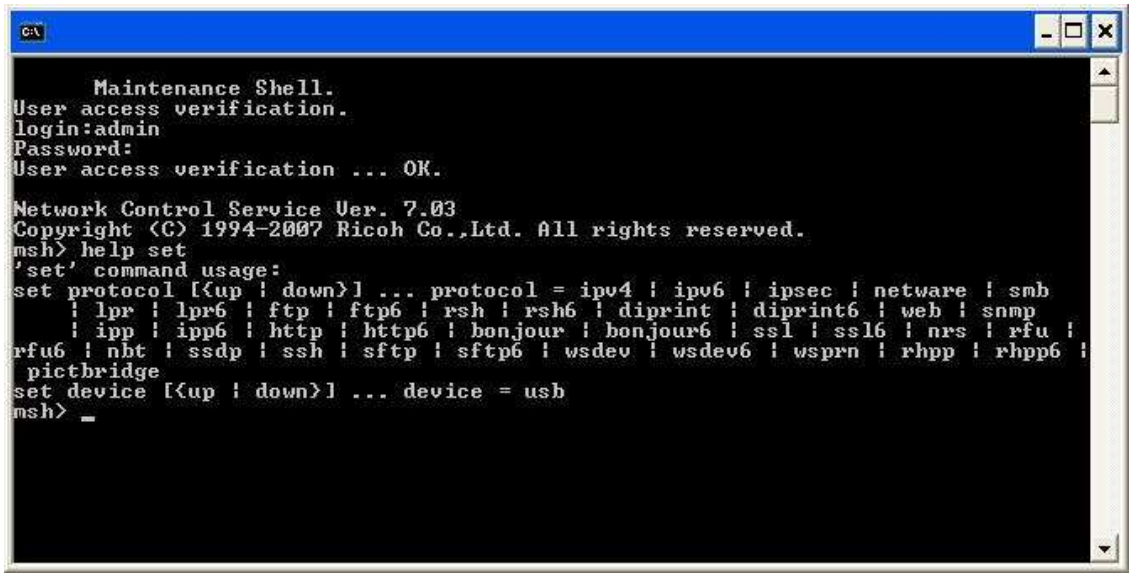
RFU	10021	-	-	Y	Y	If this port is closed, remote firmware update will still be available via ftp. However, if RFU is to be used, we recommend keeping this port open as the ftp password is sent in clear text.
RHPP	59100	Y	Y	Y	Y	If this port is closed, RHPP is not available.
IPDS	5001	Y	-	Y	-	
WS Discovery / WS Device	3702 53000	Y	Y	Y	Y	When either WS Device or WS Printer is disabled via Web Image Monitor or mshell, these ports are both closed.
WS Printer	53001	Y		Y		

3-3 Disabling Services – Web Image Monitor

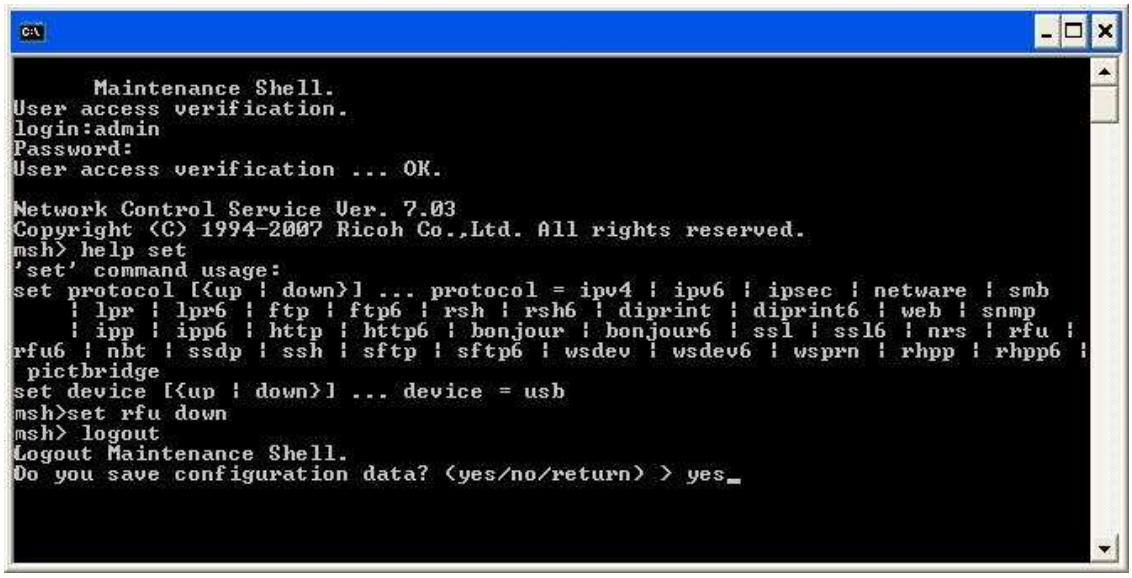


3-3-1 Disabling Services – mshell

Set <service> up/down

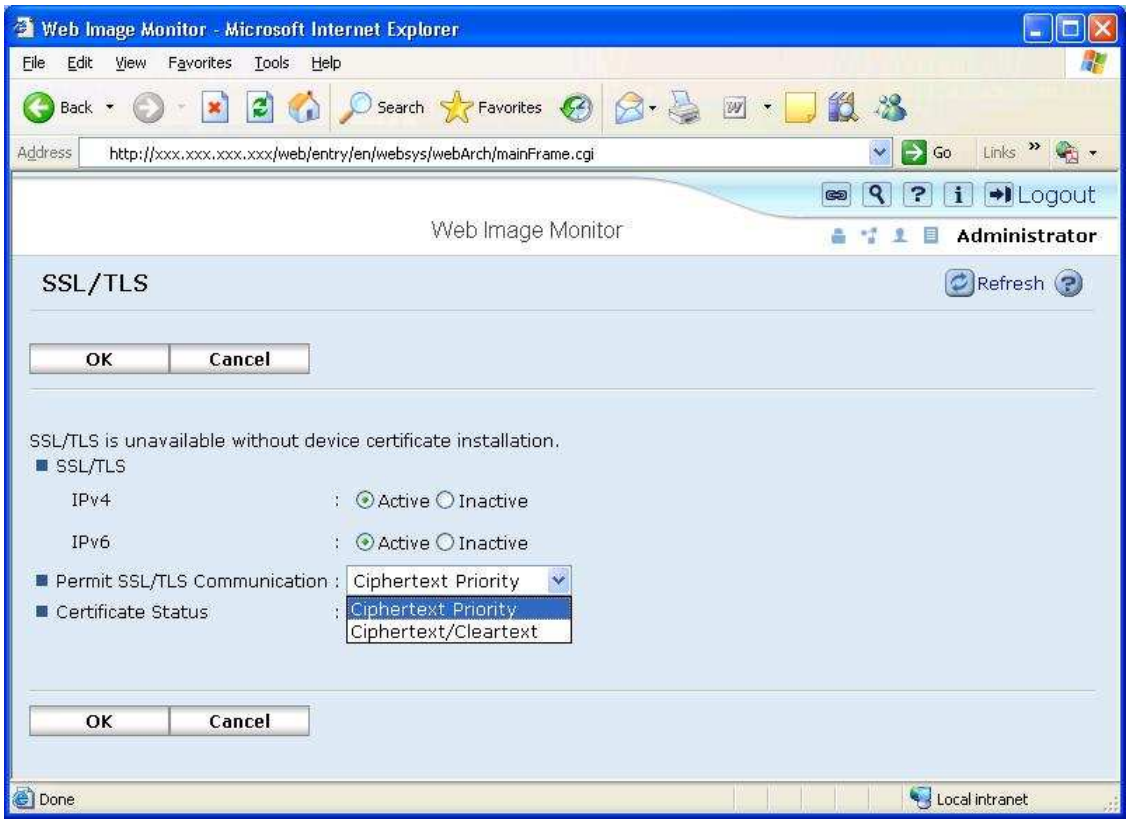

Maintenance Shell.
User access verification.
login:admin
Password:
User access verification ... OK.
Network Control Service Ver. 7.03
Copyright (C) 1994-2007 Ricoh Co.,Ltd. All rights reserved.
msh> help set
'set' command usage:
set protocol [<up | down>] ... protocol = ipv4 | ipv6 | ipsec | netware | smb
| lpr | lpr6 | ftp | ftp6 | rsh | rsh6 | diprint | diprint6 | web | snmp
| ipp | ipp6 | http | http6 | bonjour | bonjour6 | ssl | ssl6 | nrs | rfu |
rfu6 | nbt | ssdp | ssh | sftp | sftp6 | wsdev | wsdev6 | wsprn | rhpp | rhpp6 |
pictbridge
set device [<up | down>] ... device = usb
msh>

After saving, the user will be prompted to save or discard changes.


Maintenance Shell.
User access verification.
login:admin
Password:
User access verification ... OK.
Network Control Service Ver. 7.03
Copyright (C) 1994-2007 Ricoh Co.,Ltd. All rights reserved.
msh> help set
'set' command usage:
set protocol [<up | down>] ... protocol = ipv4 | ipv6 | ipsec | netware | smb
| lpr | lpr6 | ftp | ftp6 | rsh | rsh6 | diprint | diprint6 | web | snmp
| ipp | ipp6 | http | http6 | bonjour | bonjour6 | ssl | ssl6 | nrs | rfu |
rfu6 | nbt | ssdp | ssh | sftp | sftp6 | wsdev | wsdev6 | wsprn | rhpp | rhpp6 |
pictbridge
set device [<up | down>] ... device = usb
msh>set rfu down
msh> logout
Logout Maintenance Shell.
Do you save configuration data? (yes/no/return) > yes

3-3-2 HTTP/HTTPS settings

Security > SSL/TLS



3-3-3 Permit SSL/TLS Communication

- Ciphertext/Clear Text: Permit both HTTPS and HTTP connections. No forwarding of HTTP to HTTPS.
- Ciphertext Priority: Any incoming HTTP request that can be forwarded to HTTPS will be forwarded. With this setting it will be possible to use HTTPS from Internet Explorer, Netscape Navigator, etc. (HTTP will be forwarded) but not using IPP from SmartDeviceMonitor for Client etc. (these requests cannot be forwarded). If the request cannot be forwarded to HTTPS, HTTP will be permitted.
- Ciphertext Only: Permit only HTTPS connections. All incoming HTTP requests will be forwarded to HTTPS. If the request cannot be forwarded, the connection will be rejected.

HTTP/HTTPS settings

Security > SSL/TLS

In addition to the features described on the previous page, this feature is new.

NOTE:

The new features will only appear if specific versions of the firmware are applied:

MFP Model	Network Support	Web Support
D017/D018/D019/D020	7.34 or later	1.60 or later
D084/D085	7.34 or later	1.04 or later
D009/D011/D012/D013	7.16 or later	1.32.1 or later
D091/D092	7.34 or later	1.54 or later
D014/D015	7.34 or later	1.05 or later

Printer Model	Network Support	Web Support	Printer Support
G179	7.34	1.14	1.18

Q: What has been changed?

A: Implementation of some of the NIST recommendations for cryptographic algorithms and key lengths (outlined in SP 800-131).

NIST SP 800-131

- **http://csrc.nist.gov/publications/drafts/800-131/draft-sp800-131_spdjune2010.pdf**

- **The ability to enable/disable specific versions of SSL/TLS:**
- **Support for certificate signing using an RSA key length of 2048 bits.**

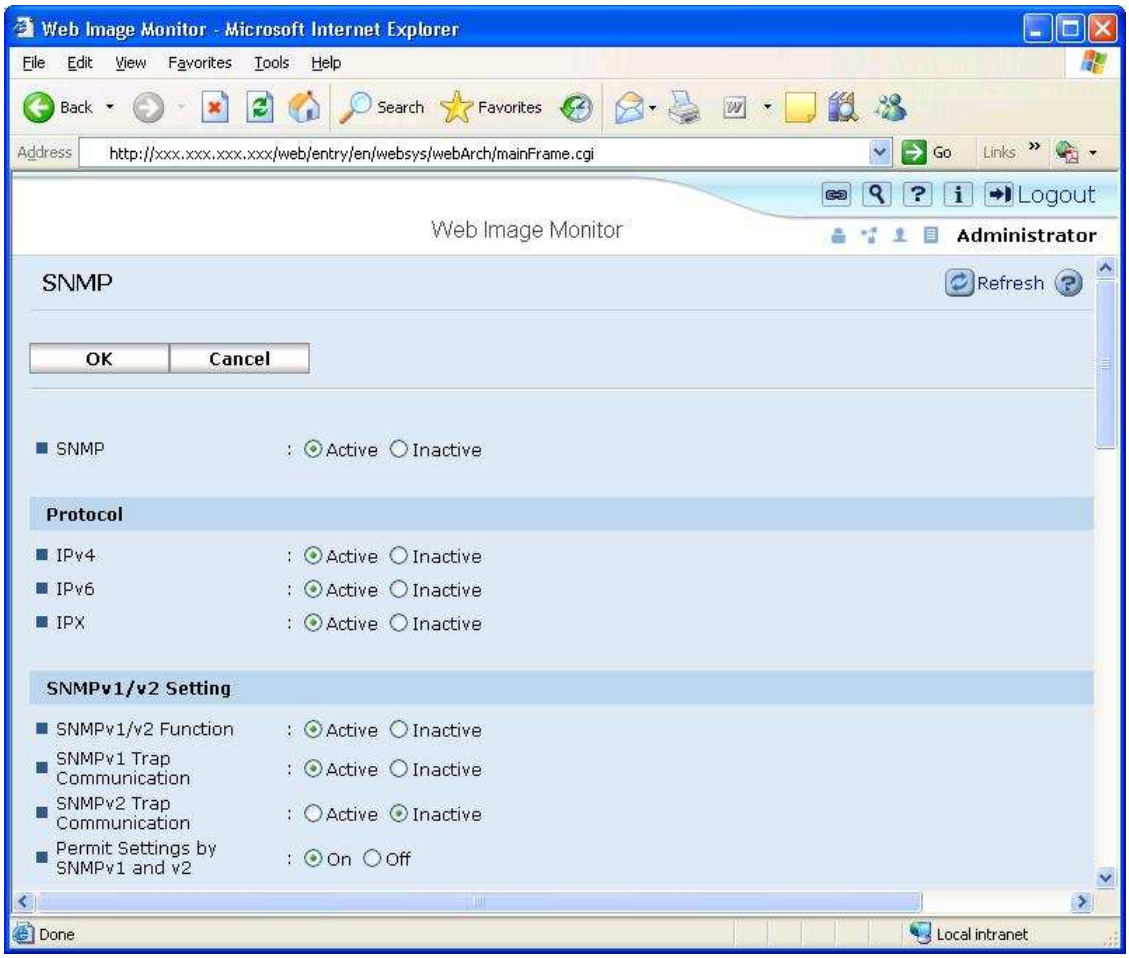
- **Support for RSA encryption with a key length of 2048 bits (used for SSL).**
    - 512 bits (md5WithRSA)
    - 1024 bits (sha1WithRSA)
    - 2048 bits (sha1WithRSA)
        - ✧ Support for 2048 bit RSA was implemented in response to the NIST SP 800-131 recommendations.
- **The ability to enable/disable specific symmetric-key encryption algorithms/key lengths.**

Encryption Strength Setting
AES : 128bit 256bit
3DES : 168bit
DES : 40bit 56bit
RC4 : 40bit 56bit 64bit 128bit
RC2 : 40bit 56bit 128bit

3-4 SNMP settings:

3-4-1 Web Image Monitor

To access the SNMP (v1/v2) settings, click Network > SNMP.



- **SNMP**

(This setting can be configured either from here or from the SNMPv3 settings.)
Enable: Opens the SNMP port
Disable: Closes the port completely. No SNMP communication of any version can be used.

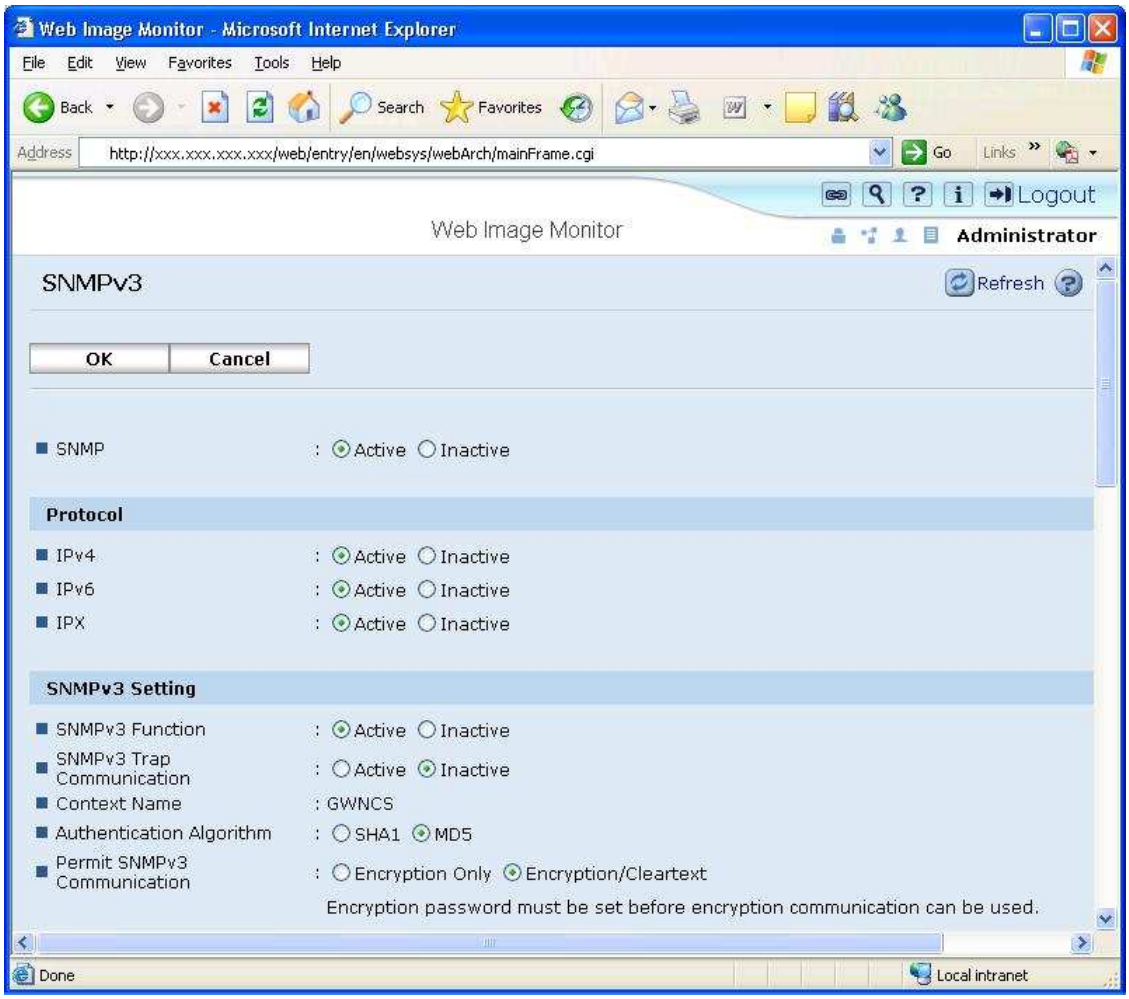
- **SNMP v1/v2 Function**

Enable: Allows the use of SNMP v1/v2.
Disable: Does not allow connections using SNMP v1/v2. This is recommended because SNMP v1/v2 doesn't have any mechanism for encryption or authentication, we recommend using 'Disable' for this setting unless absolutely necessary.

- **Permit Settings by SNMP v1 and v2**

On: This enables SNMP set. It is used to write changes to settings.
Off: This disables SNMP set. Only get will be permitted. Therefore, settings can be read but not changed.

3-5 Network > SNMP v3



- **SNMP**

(This setting can be configured either from here or from the SNMPv1/v2 settings.)
Enable: Opens the SNMP port
Disable: Closes the port completely. No SNMP communication of any version can be used.

- **SNMP v3 Function Enable:**

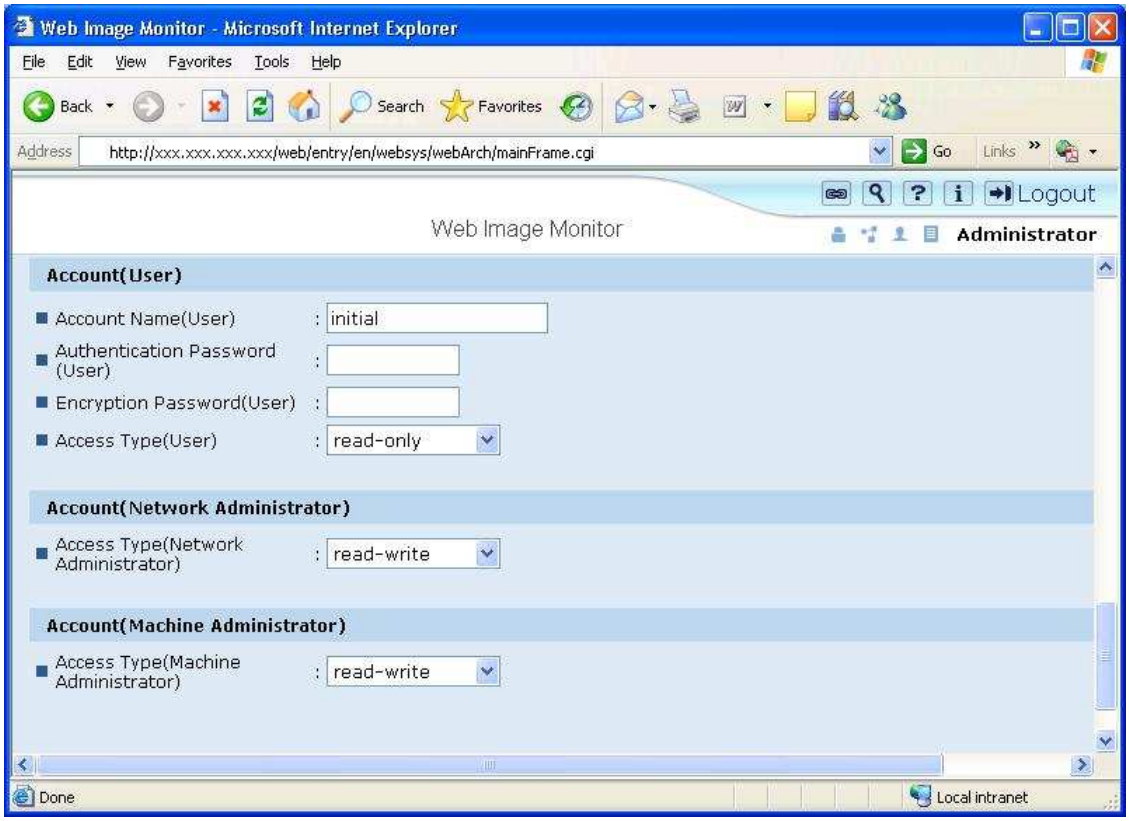
Allows communication using SNMP v3. Disable: Does not allow communication via SNMP v3.

- **Authentication Algorithm**

SHA1: Hashes the username and password using the SHA1 hashing algorithm.
MD5: Hashes the username and password using the MD5 hashing algorithm.

- **Permit SNMPv3 communication**

Encryption Only: The username and password must be encrypted using the hashing algorithm selected above.
Encryption/Clear Text: The username and password can be sent either encrypted or unencrypted.



There are 3 different types of accounts that can be used for SNMPv3 connections. Only the User account can be fully configured here. For information about fully configuring the Machine and Network Administrator accounts, please refer to the Appendix section entitled “Administrator Account Settings”.

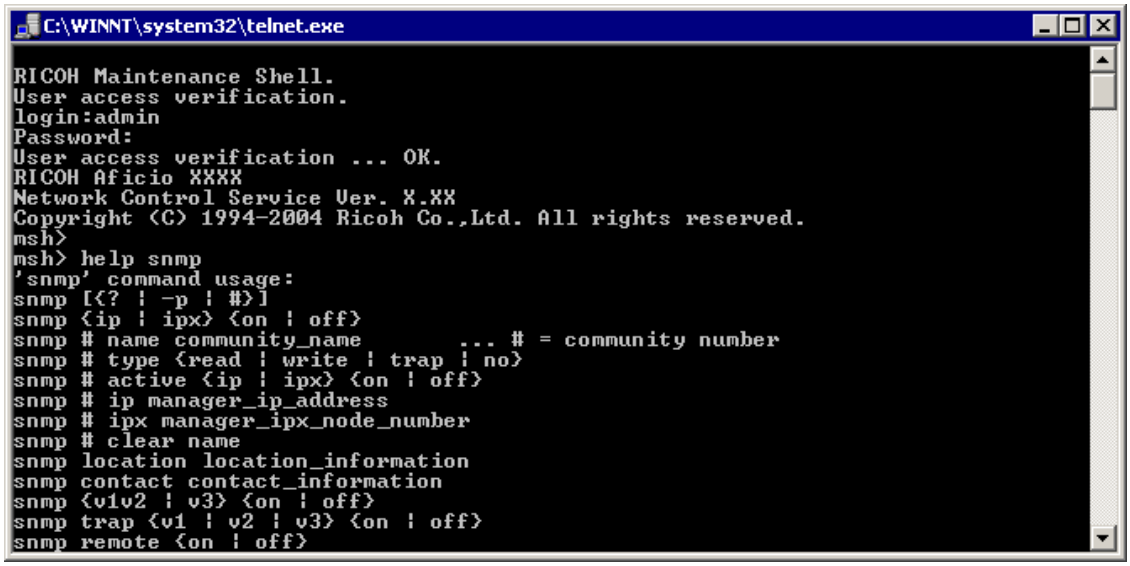
Account Name (User): This is the username that the user will use to login to SNMPv3.

Authentication Password (User): This is the password that the user will use to login to SNMPv3.

Encryption Password (User): This is the key used for SHA1 or MD5 hashing of the username and password.

3-6 Mshell

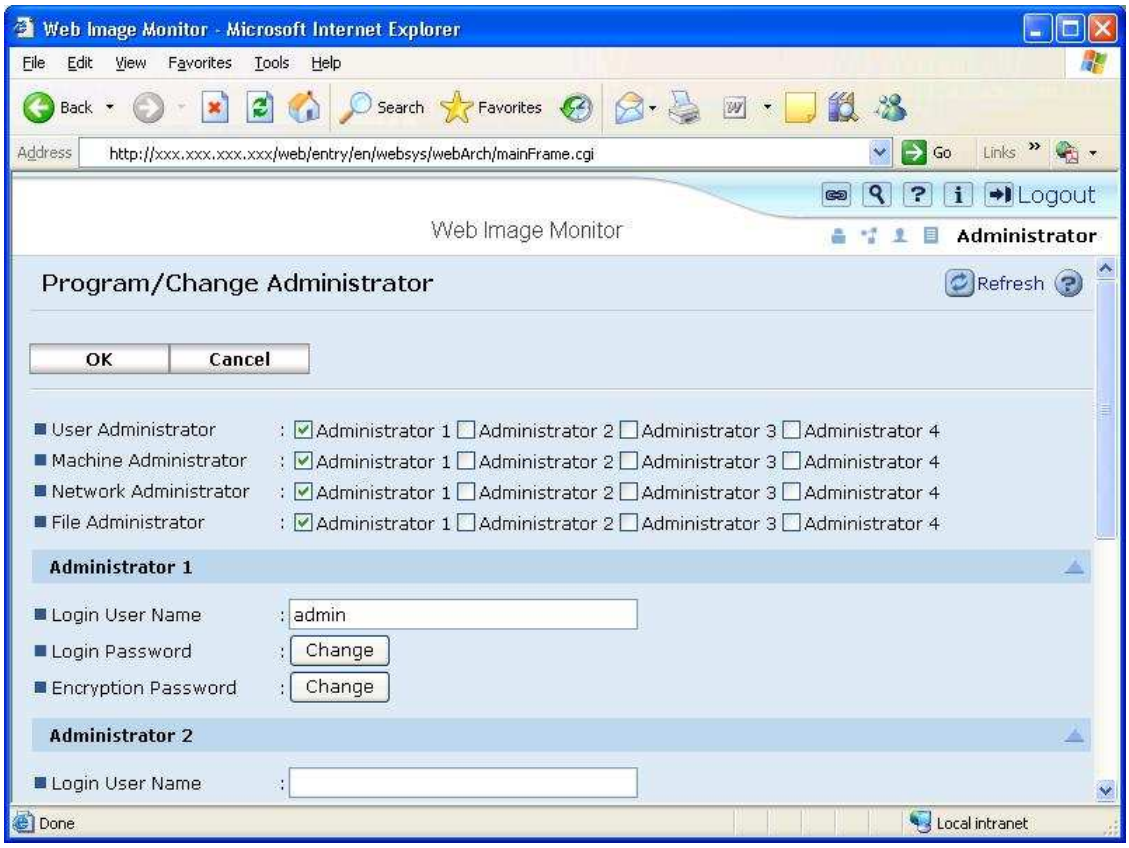
You can configure SNMP settings using snmp commands from mshell. These commands can be displayed by typing ‘help snmp’ in mshell.



3-7 Administrator Account Settings

3-7-1 Web Image Monitor

Device Settings > Program/Change Administrator


Web Image Monitor - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://xxx.xxx.xxx.xxx/web/entry/en/websys/webArch/mainFrame.cgi
Go Links
Logout
Web Image Monitor
Administrator
Program/Change Administrator
Refresh
OK
Cancel
User Administrator : Administrator 1 Administrator 2 Administrator 3 Administrator 4
Machine Administrator : Administrator 1 Administrator 2 Administrator 3 Administrator 4
Network Administrator : Administrator 1 Administrator 2 Administrator 3 Administrator 4
File Administrator : Administrator 1 Administrator 2 Administrator 3 Administrator 4
Administrator 1
Login User Name : admin
Login Password : Change
Encryption Password : Change
Administrator 2
Login User Name :
Done
Local intranet

MFP Administrator account settings can be changed from here. Administrator roles can be assigned to any or all of up to 4 Administrators.

These settings affect the Administrator logins for TELNET, Web Image Monitor and SNMP v3.

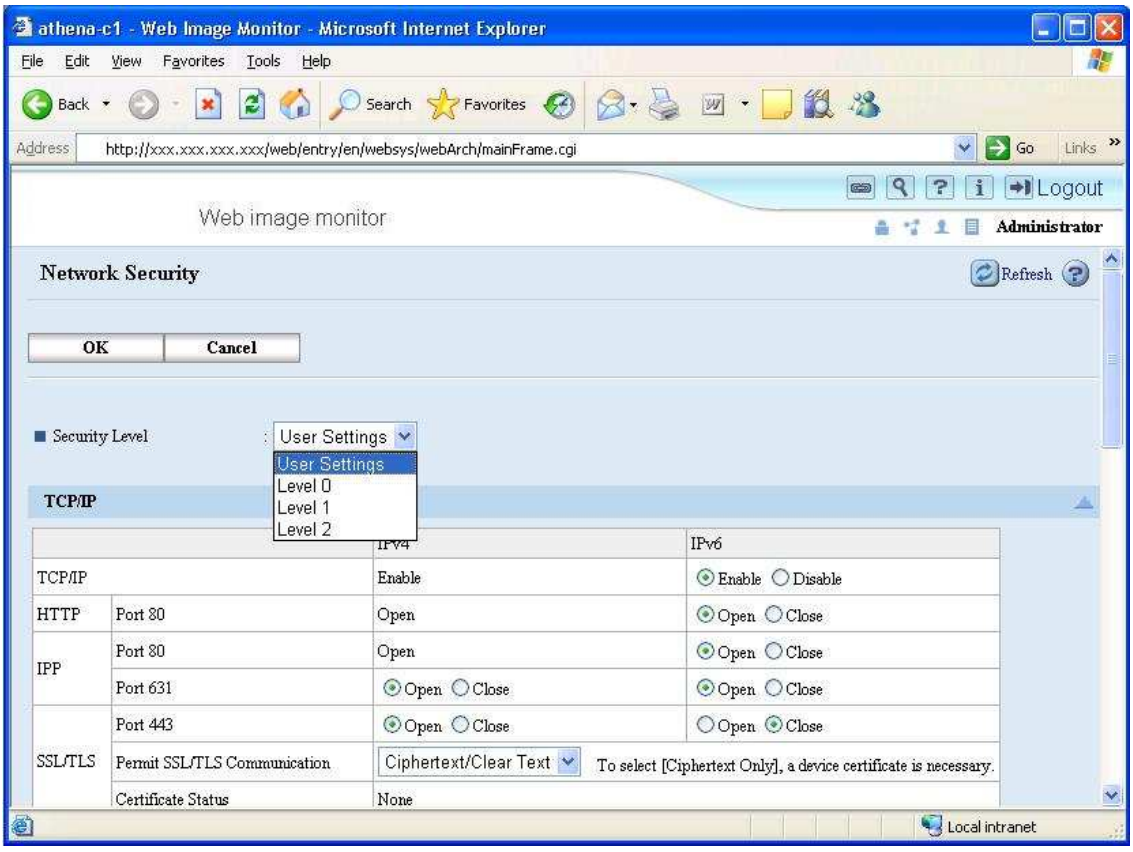
3-8 Network Security Level Settings

3-8-1 Configuration

Network Security Levels are settings or files designed to meet different levels of security in customer environments. The advantage to the Network Security Level settings is that they make the task of configuration easier. Customers can use the Network Security levels as is, or modify them to suit their needs. There are 3 levels to choose from:

[Level 2] – Maximum security.
[Level 1] – Moderate security for use in an office LAN.
[Level 0] – Basic security for closed environments.
[User Settings] – Manually defined settings.

To access the Network Security Level setting, click ‘Security’ -> ‘Network Security’.



3-8-2 Description of the Levels:

	Setting		Network Security Level		
			Level 0	Level 1	Level 2
Interface	IEEE 1394 SBP-2		Enabled	Enabled	Disabled
	Bluetooth		Enabled	Enabled	Disabled
	IP over 1394		Enabled	Enabled	Enabled
TCP/IP	TCP/IP		Enabled	Enabled	Enabled
	HTTP/HTTPS	Port 80	Port open	Port open	Port open*1
		Port 443	Port open	Port open	Port open
		Port 7443/7444	Port open	Port open	Port open
	IPP	Port 80	Port open	Port open	Port open *1
		Port 443	Port open	Port open	Port open
		Port 631	Port open	Port open	Port closed
	SSL	Encryption Mode	Ciphertext Priority	Ciphertext Priority	Ciphertext Only *2
	DIPRINT	Port 9100	Port open	Port open	Port closed
	LPR	Port 515	Port open	Port open	Port closed
	FTP	Port 21	Port open	Port open	Port open
	SSH/SFTP	Port 22	Port open	Port open	Port open
	RFU	Port 10021	Port open	Port open	Port open
	RSH/RCP	Port 514	Port open	Port open	Port closed
	SNMP	Port	Port open	Port open	Port open
		SNMP v1/v2 (Read)	Enabled	Enabled	Disabled
		SNMP v1/v2 (Write)	Enabled	Disable	Disabled
		SNMP v3	Enabled	Enabled	Enabled
		SNMP v3 with Encrypt	Automatic	Automatic	Ciphertext Only
	TELNET	Port 23	Port open	Port closed	Port closed
	SSDP (UPnP)	Port 1900	Port open	Port open	Port closed
	mDNS	Port 5353	Port open	Port open	Port closed
	NBT	Port 137/138	Port open	Port open	Port closed
	SMB	Port 139	Port open	Port open	Port closed
	WS-Device	Port 3702/53000	Port open	Port open	Port closed
	WS-Printer	Port 53001	Port open	Port open	Port closed
	RHPP	Port 59100	Port open	Port open	Port closed
	IPDS	Port 5001	Port open	Port open	Port closed
Netware	Netware		Enabled	Enabled	Disabled
AppleTalk	AppleTalk		Enabled	Enabled	Disabled

*1: The port is open but cannot be used to access the web service because the SSL setting is Ciphertext Only.

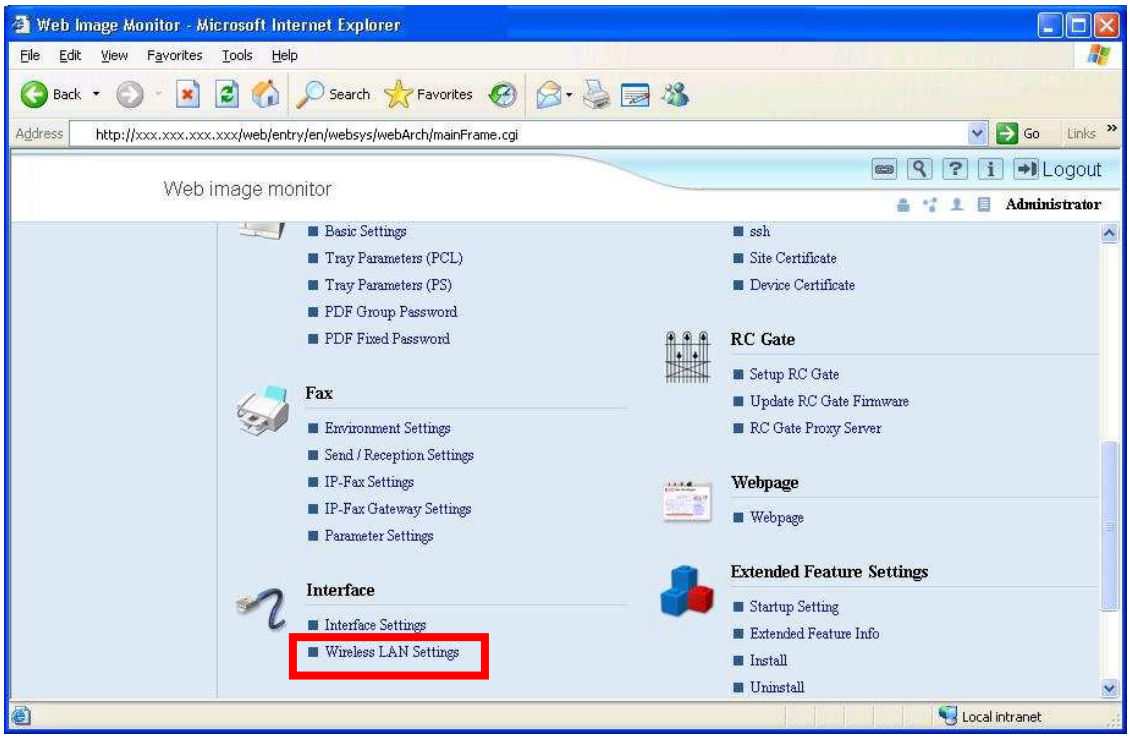
*2: If the SSL setting is Ciphertext only, the products will still accept IPP jobs using port 80.

3-9 Wireless LAN settings

WEP, WPA-PSK/WPA2-PSK, and WPA (802.1X)/WPA2 (802.1X) can be configured via the operation panel, telnet, or Web Image Monitor. However, the WPA (802.1X)/WPA2 (802.1X) certificate settings can only be configured in Web Image Monitor.

3-9-1 Web Image Monitor

Click 'Interface' -> 'Wireless LAN Settings'.

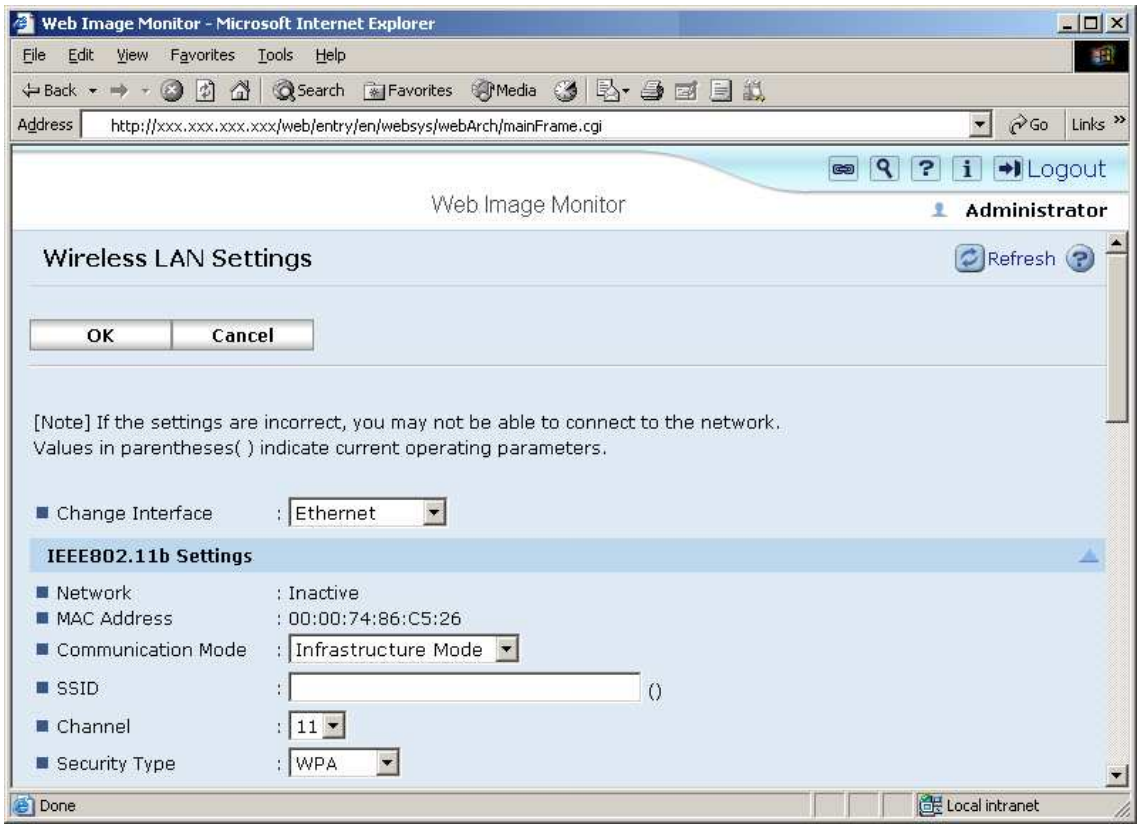


- Change Interface Ethernet: Enable Ethernet IEEE802.11b: Enable IEEE802.11b

3-9-2 [IEEE802.11b Settings]

- Network Enable: IEEE802.11b is enabled Disable: IEEE802.11b is disabled
- MAC Address

Displays the MAC Address of the Wireless LAN board



- Communication Mode

  802.11 Ad-hoc Mode: Ad-hoc connection using SSID.

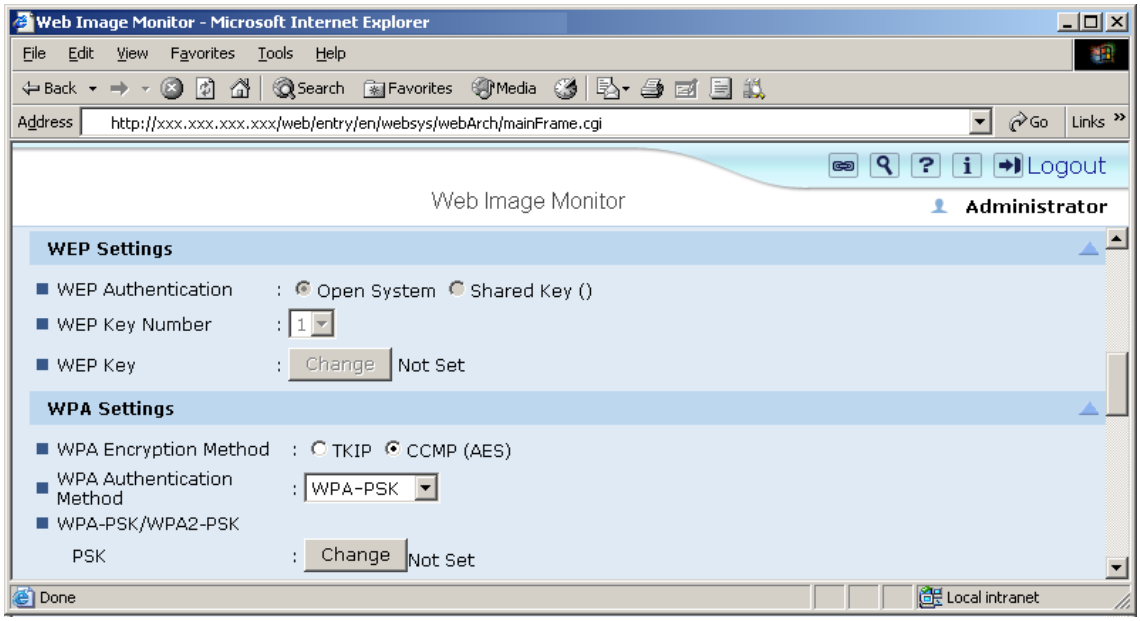
  Ad-hoc Mode: Ad-hoc connection without using SSID.

  Infrastructure Mode: Communicates using an access point and SSID.

- Channel

Sets the radio frequency used. If Infrastructure mode is being used, this setting is unimportant as the channel defined by the access point will be used automatically.

- Security Type
  - Inactive: No encryption of data.
  - WEP: Uses WEP security.
  - WPA: Uses WPA security.



3-9-3 WEP

WEP settings can only be configured if 'WEP' is selected in 'IEEE802.11b Settings' -> 'Security Type'.

- WEP Authentication

  Open System: Anyone with the correct SSID can join the network.

NOTE: As the system uses a WEP key, simply joining the network is not enough to be able to receive or send readable communications.

  Shared Key: WEP key required to join the network.

- WEP Key Number

Up to four WEP keys can be saved in the MFP. Select one of them.

- WEP Key

Set the WEP key used for WEP encryption. If 64-bit key is used, 10 hexadecimal characters or 5 alphanumeric characters need to be entered. If a 128-bit key is used, 26 hexadecimal characters or 13 alphanumeric characters need to be entered.

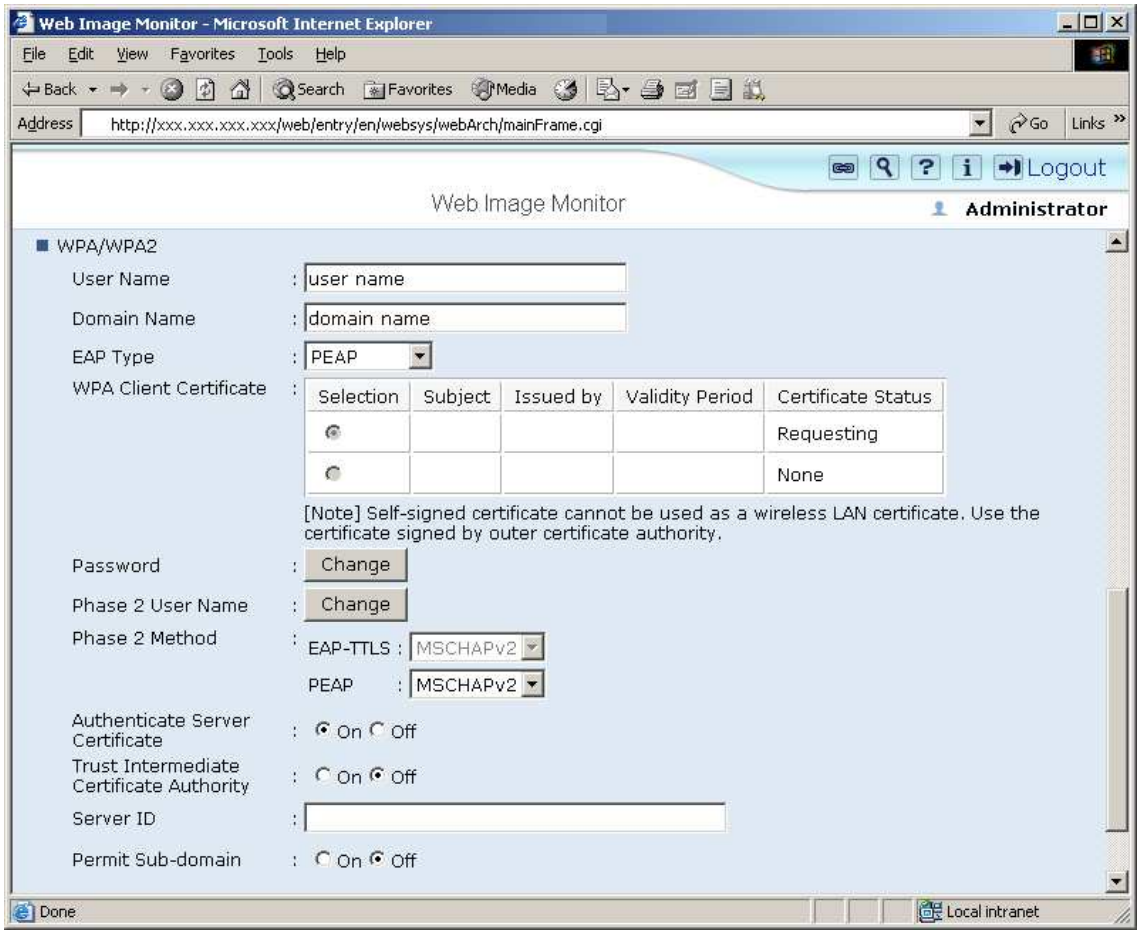
3-9-4 WPA

WPA settings can only be configured if 'WPA' is selected in 'IEEE802.11b Settings' -> 'Security Type'.

- WPA Encryption Method TKIP: Uses TKIP. CCMP: Uses CCMP.
- WPA Authentication Method
  - WPA: Uses WPA (802.1X).
  - WPA2: Uses WPA2 (802.1X)
  - WPA-PSK: Uses WPA-PSK.
  - WPA2-PSK: Uses WPA2-PSK.

- WPA-PSK/WPA2-PSK

PSK: Sets the pre-shared key used.

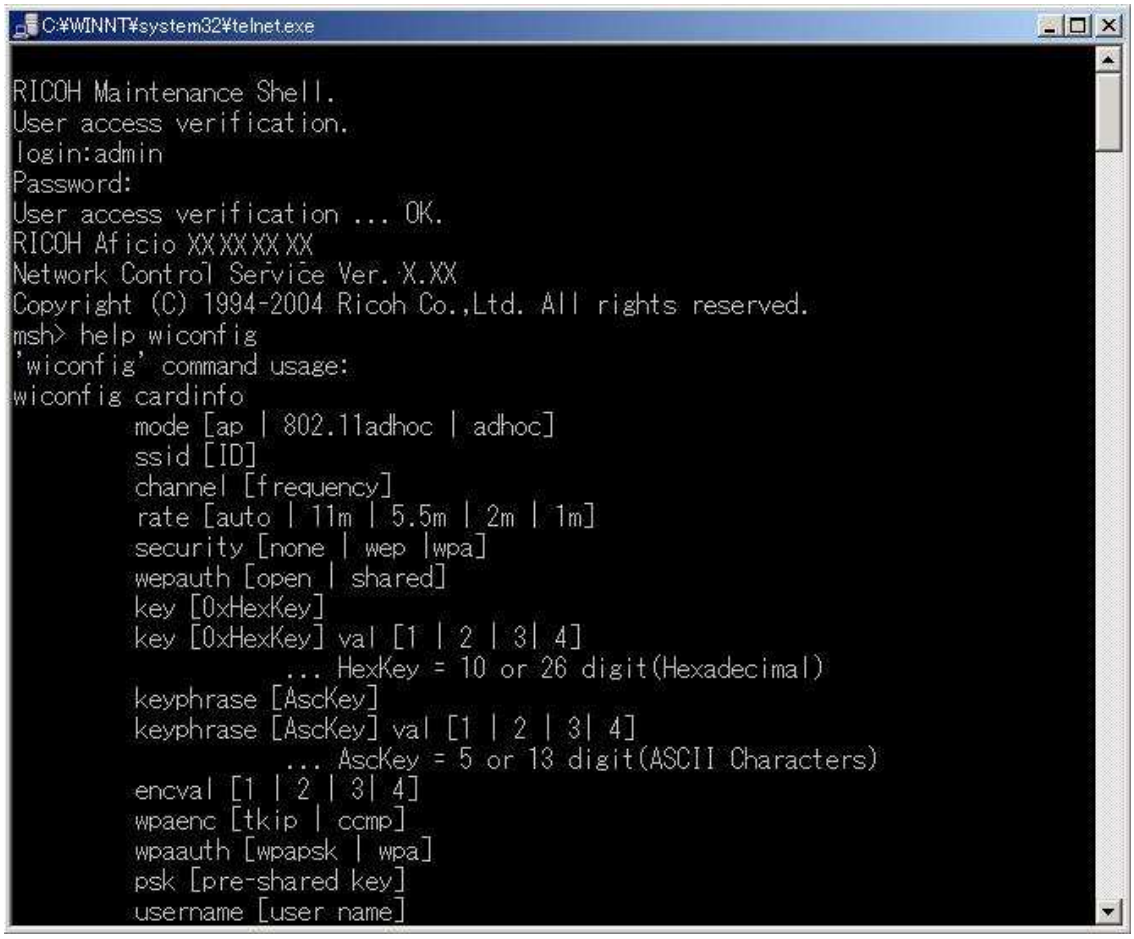


WPA/WPA2

- User Name: This is the username used for EAP authentication on the Radius server.
- Domain Name: This is the domain name used for the authentication on the Radius server.
- EAP Type: EAP-TLS, LEAP, EAP-TTLS, or PEAP
- WPA Client Certificate: WPA/WPA2 802.1X certificate.
- Password: This is the password used for EAP authentication on the Radius server.
- Phase 2 User Name: This is the user name used in phase 2 of EAP-TTLS and PEAP.
- Phase 2 Methods (EAP-TTLS): If EAP-TTLS is selected as the EAP type a Phase2 authentication method must be selected. Select from CHAP, MSCHAP, MSCHAPv2, PAP, or MD5
- Phase 2 Methods (PEAP): If PEAP is selected as the EAP type, a Phase2 authentication method must be selected. Select from MSCHAPv2 or TLS.
- Authentication Server Certificate: Select whether the Radius Server is required to send a certificate to connecting WPA (802.1x) client.
- Trust Intermediate Certificate Authority: Select whether the certificate provided by the Radius Server must be signed by a trusted CA.
- Server ID: This is the CN (or the DC) of server certificate.
- Permit Sub-domain: Select whether the server certificate is permitted for the sub-domain of server ID.

3-9-5 mshell

Configure Wireless LAN settings using ‘wiconfig’ commands from mshell. For a list of commands, type ‘help wiconfig’ in mshell.

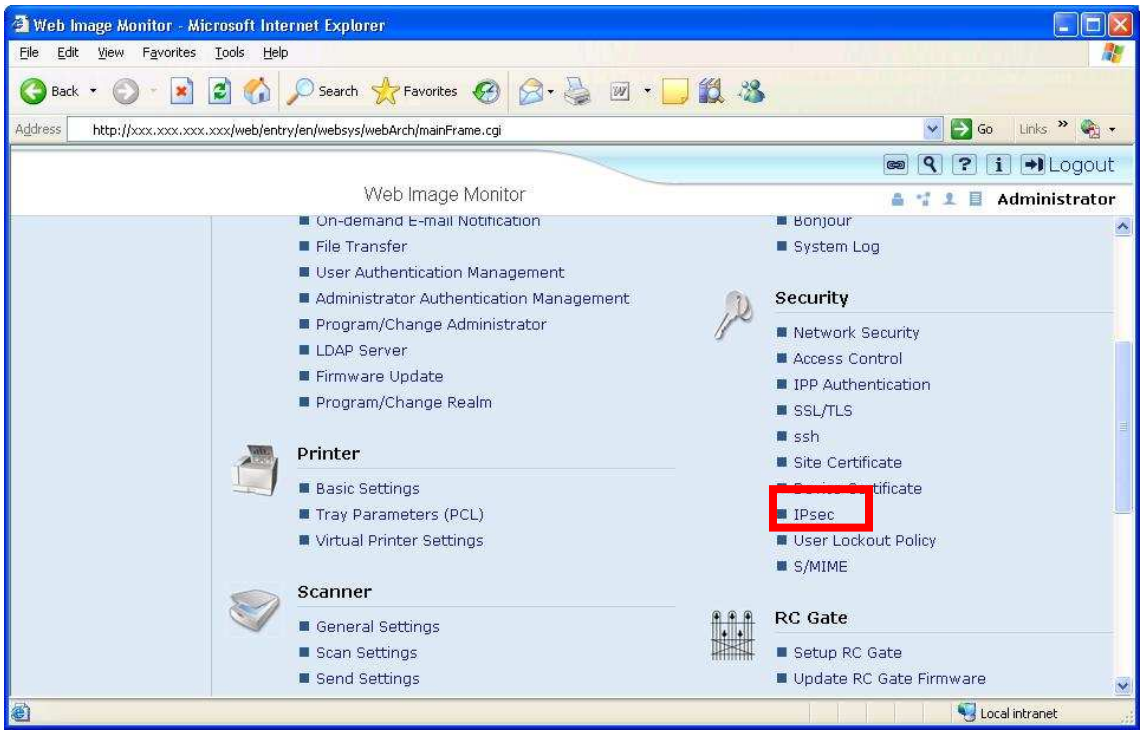

C:¥WINNT¥system32¥telnet.exe
RICOH Maintenance Shell.
User access verification.
login:admin
Password:
User access verification ... OK.
RICOH Aficio XXXXXXXX
Network Control Service Ver. X.XX
Copyright (C) 1994-2004 Ricoh Co.,Ltd. All rights reserved.
msh> help wiconfig
'wiconfig' command usage:
wiconfig cardinfo
mode [ap | 802.11adhoc | adhoc]
ssid [ID]
channel [frequency]
rate [auto | 11m | 5.5m | 2m | 1m]
security [none | wep |wpa]
wepauth [open | shared]
key [0xHexKey]
key [0xHexKey] val [1 | 2 | 3| 4]
... HexKey = 10 or 26 digit(Hexadecimal)
keyphrase [AscKey]
keyphrase [AscKey] val [1 | 2 | 3| 4]
... AscKey = 5 or 13 digit(ASCII Characters)
encval [1 | 2 | 3| 4]
wpaenc [tkip | ccmp]
wpaauth [wpapsk | wpa]
psk [pre-shared key]
username [user name]

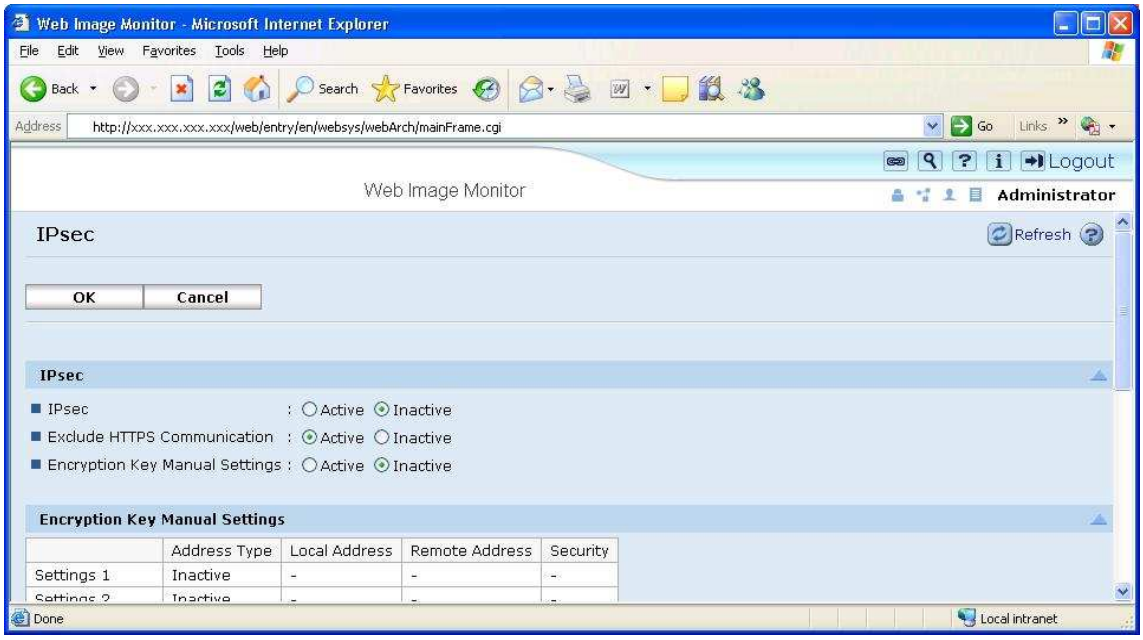
3-9-6 IPsec Settings

IPsec settings can be configured via telnet, or Web Image Monitor. In order to establish IPsec connection in this section, we focus on MFP configuration only. Please refer to the client's manual for information about configuring it

3-9-7 Web Image Monitor

Security > IPsec



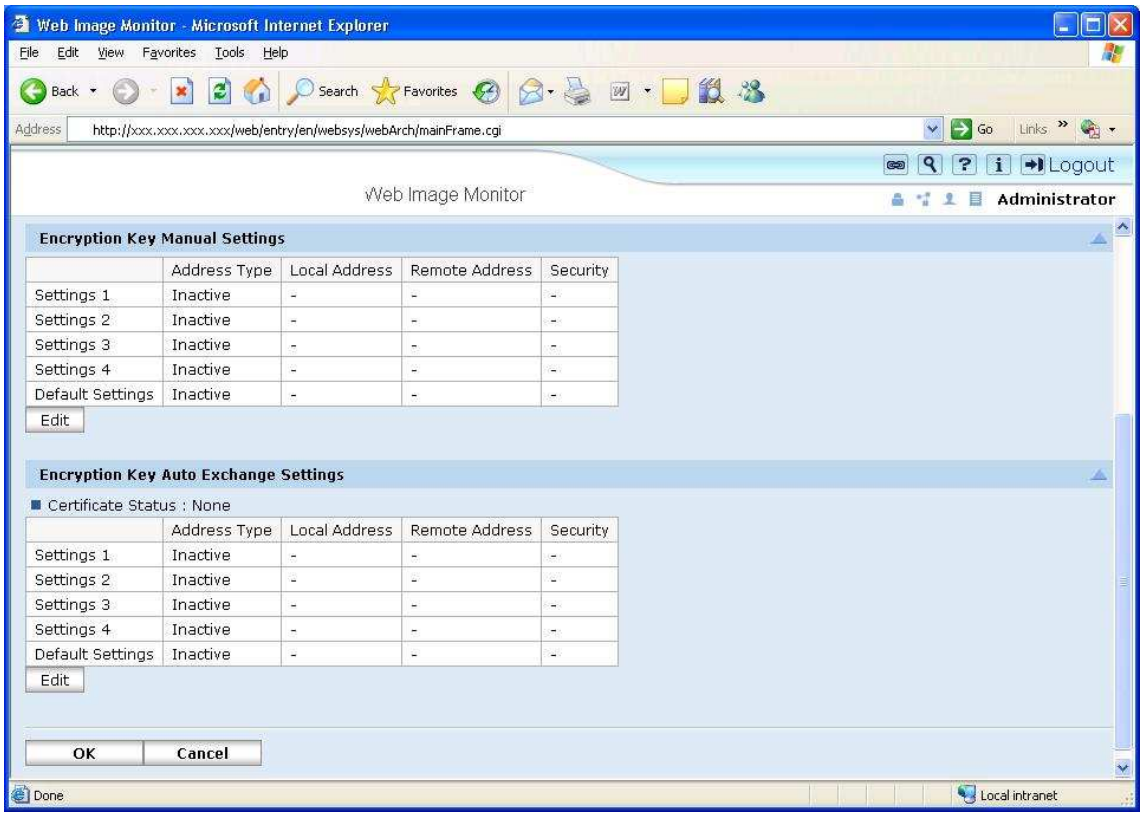


IPsec:

- IPsec
  Active: Activate IPsec
  Inactive: Deactivate IPsec

- Exclude HTTPS Communication
  Active: Exclude HTTPS Communication for IPsec policy
  Inactive: Do not exclude HTTPS communication for IPsec policy

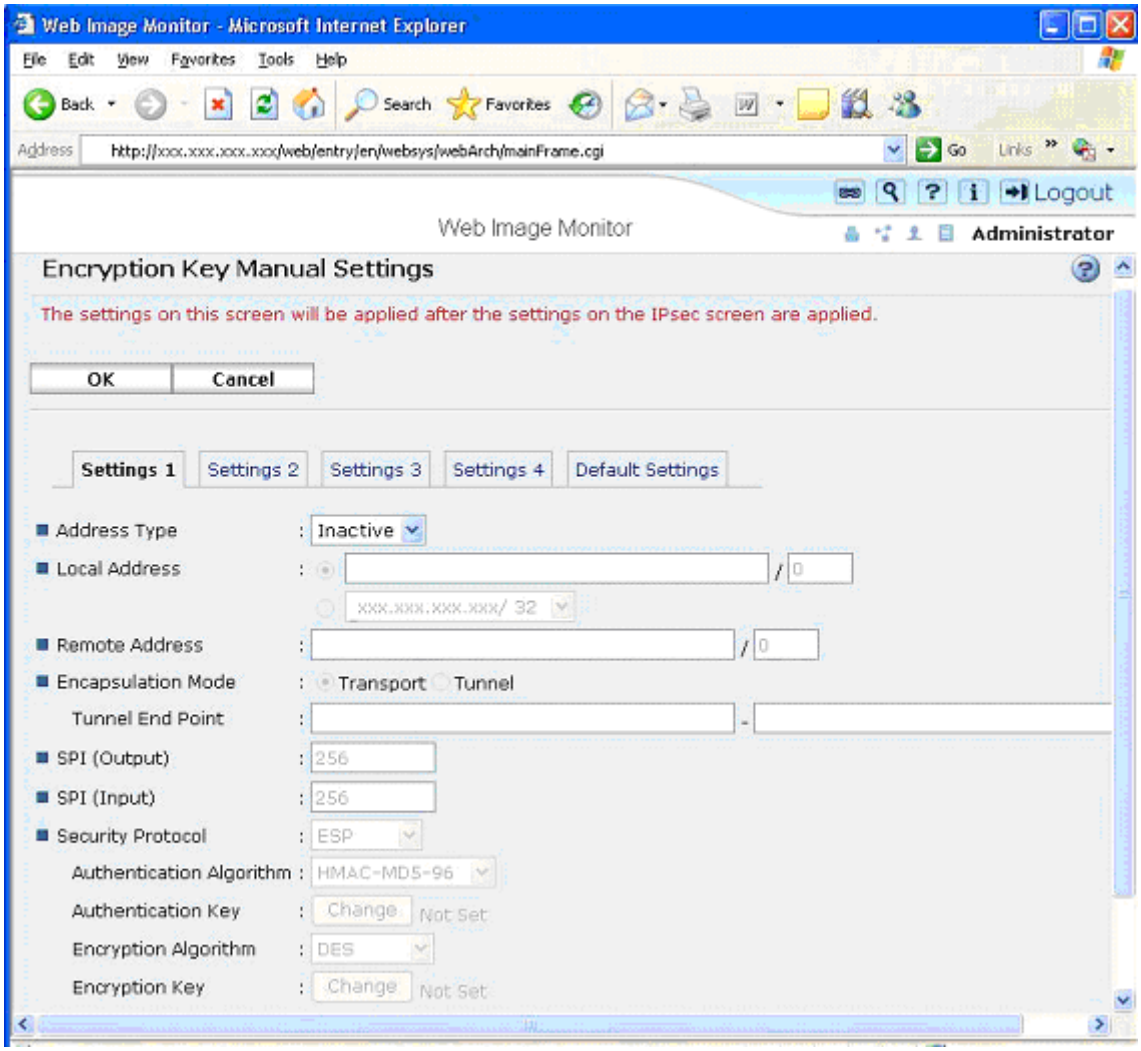
- Encryption Key Manual Settings
  Active: When specifying SA parameters manually, select Active.
  Inactive: When specifying SA parameters automatically, select Inactive


Web Image Monitor - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://xxx.xxx.xxx.xxx/web/entry/en/websys/webArch/mainFrame.cgi
Go Links
Logout
Web Image Monitor
Administrator
Encryption Key Manual Settings
Address Type Local Address Remote Address Security
Settings 1 Inactive - - -
Settings 2 Inactive - - -
Settings 3 Inactive - - -
Settings 4 Inactive - - -
Default Settings Inactive - - -
Edit
Encryption Key Auto Exchange Settings
Certificate Status : None
Address Type Local Address Remote Address Security
Settings 1 Inactive - - -
Settings 2 Inactive - - -
Settings 3 Inactive - - -
Settings 4 Inactive - - -
Default Settings Inactive - - -
Edit
OK
Cancel
Done
Local intranet

Encryption Key Manual Settings:
To configure IPsec SA parameters manually, click ‘Edit’.

Encryption Key Auto Exchange Settings:
To configure IPsec SA Parameters automatically, click ‘Edit’.

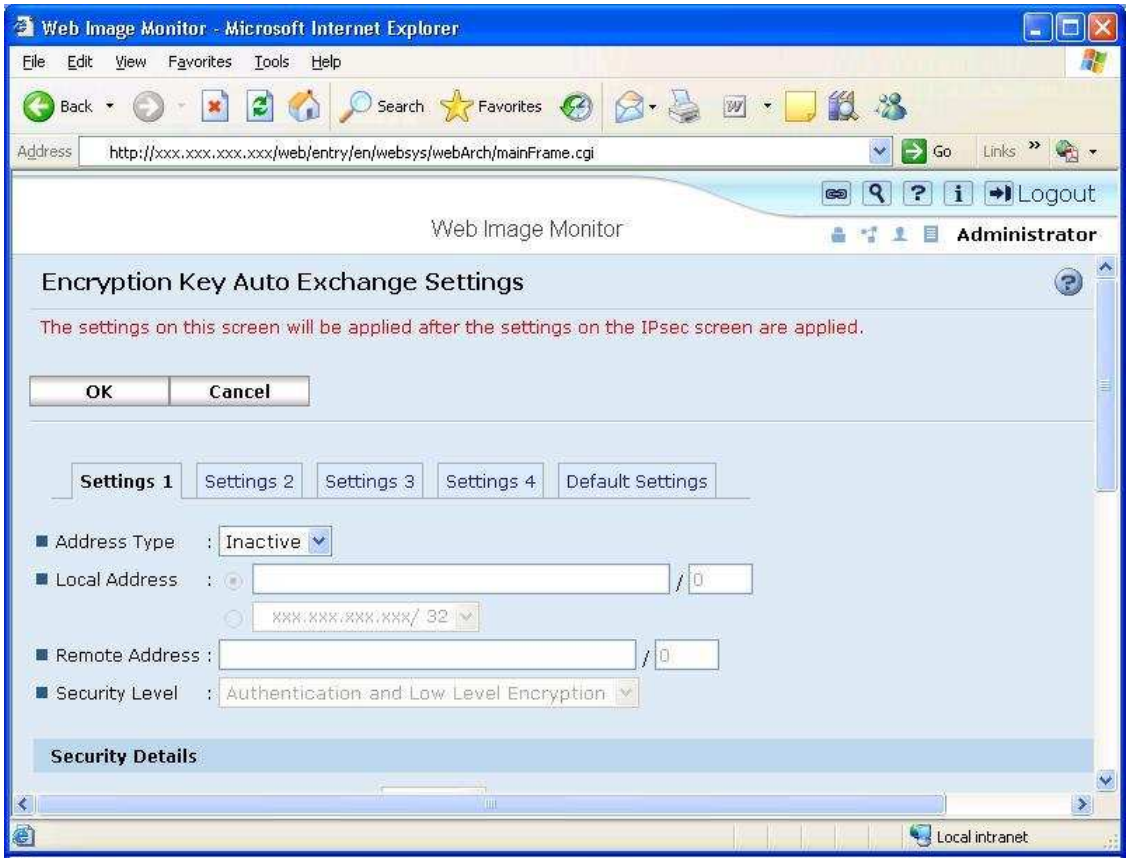
The Settings are listed in order of priority top to bottom (‘Settings 1’, ‘Settings 2’, ‘Settings 3’, ‘Settings 4’, ‘Default Settings’) The lowest number has the highest priority. ‘Default Settings’ has the lowest priority.



Encryption Key Manual Settings:

- Address Type
  - Inactive: Do not use IPsec
  - IPv4: Apply IPsec for IPv4
  - IPv6: Apply IPsec for IPv6
  - IPv4/IPv6: Apply IPsec for IPv4 and IPv6 (Only available for 'Default Settings')
- Local Address: Enter (Select) the product's IP address.
- Remote Address: Enter the counterpart's IP address or address range.
- Encapsulation Mode
  - Transport: IPsec is applied as Transport mode.
  - Tunnel: IPsec is applied as Tunnel mode. When Tunnel Mode is specified, Tunnel End Point has to be specified. In the left box, enter the product's IP address. In the right box, enter the gateway IP address.
- SPI (Output): Set the SPI value for outgoing SA connection. Any number between 256 and 4095
- SPI (Input): Set the SPI value for incoming SA connection. Any number between 256 and 4095

- Security Protocol
  ESP: Uses ESP
  AH: Uses AH
  AH+ESP: Uses dual mode (AH + ESP)
- Authentication Algorithm: Select from HMAC-MD5-96 or HMAC-SHA1-96 as hashing algorithm
- Authentication Key: Set the Authentication key used for hashing. For HMAC-MD5-96, enter up to 32 in hexadecimal number, or up to 16 ASCII. For HMAC-SHA1-96, enter up to 40 in hexadecimal number, or up to 20 ASCII
- Encryption Algorithm: Select from Clear Text, DES, 3DES, AES-128, AES-192, or AES-256.
- Encryption Key: Set the encryption key. If AH is selected as security protocol, this is grayed out. For DES, enter up to 16 in hexadecimal number, or up to 8 ASCII. For 3DES, enter up to 48 in hexadecimal number, or up to 24 ASCII. For AES-128, enter up to 32 in hexadecimal number, or up to 16 ASCII. For AES-192, enter up to 48 in hexadecimal number, or up to 24 ASCII. For AES-256, enter up to 64 in hexadecimal number, or up to 32 ASCII.


Web Image Monitor - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://xxx.xxx.xxx.xxx/web/entry/en/websys/webArch/mainFrame.cgi
Go Links
Logout
Web Image Monitor
Administrator
Encryption Key Auto Exchange Settings
The settings on this screen will be applied after the settings on the IPsec screen are applied.
OK Cancel
Settings 1 Settings 2 Settings 3 Settings 4 Default Settings
Address Type : Inactive
Local Address :
Remote Address :
Security Level : Authentication and Low Level Encryption
Security Details
Local intranet

Encryption Key Auto Exchange Settings:

- Address Type
  Inactive: Do not use IPsec
  IPv4: Apply IPsec for IPv4
  IPv6: Apply IPsec for IPv6
  IPv4/IPv6: Apply IPsec for IPv4 and IPv6 (Only available for 'Default Settings')
- Local Address: Enter (Select) the product's IP address.
- Remote Address: Enter the counterpart's IP address or address range.
- Security Level: User can select the IPsec security level from followings. Depending on the selected security level, the parameters in Security Details change.
  Authentication Only
  Authentication and Low Level Encryption
  Authentication and High Level Encryption
  User Settings

Security Details:

- Security Policy
  Apply: Apply IPsec
  Bypass: Do not apply IPsec. All data is sent as plain text.
  Discard: All data is discarded.
- Encapsulation Mode
  Transport: IPsec is applied as Transport mode.
  Tunnel: IPsec is applied as Tunnel mode. When Tunnel Mode is specified, Tunnel End Point has to be specified. In the left box, enter the product's IP address. In the right box, enter the gateway IP address.
- IPsec Requirement Level
  Use When Possible: Allows the cleartext transmission when IPsec cannot be established.
  Always Required: Allows only the IPsec transmission.
- Authentication Method
  PSK: Use pre-shared key as authentication method. If PSK is selected, the pre-shared key has to be entered up to 32 alphanumeric numbers.
  Certificate: Use certificate for authentication.

Phase 1:

- Hash Algorithm: MD5 or SHA1
- Encryption Algorithm: DES or 3DES
- Diffie-Hellman Group : Select the Diffie-Hellman Group from 1, 2, or 14
- Validity Period: Enter the number between 300 and 172800 seconds.

Phase 2:

- Security Protocol
  ESP: Uses ESP
  AH: Uses AH
  AH+ESP: Uses dual mode (AH + ESP)
- Authentication Algorithm: Select from HMAC-MD5-96 and HMAC-SHA1-96.
- Encryption Algorithm Permissions: Select from Cleartext, DES, 3DES, AES-128, AES-192, and AES-256.
- PFS
  Inactive: Do not generate the encryption or authentication keys again.
  1, 2, or 14: Diffie-Hellman Group for establishing IPsec SA in Phase 2.
- Validity Period: Enter the number between 300 and 172800 seconds.

4. Reference List

- RFC: HTTP://www.faqs.org/rfcs/
- CVE: HTTP://cve.mitre.org/
- CERT: HTTP://www.cert.org/
- CIAC: HTTP://www.ciac.org/ciac/
- Security Focus: HTTP://www.securityfocus.com/
- NESSUS: HTTP://www.nessus.org/index2.html